PheeNet

Network Access Control

User Manual ***WAS-102R***
Ver.1.00

Table of Contents

1. Before You Start **3**
1.1 Preface 3
1.2 Document Conventions 3
2. System Overview **3**
2.1 Introduction of WAS-102R 3
2.2 System Concept 4
2.3 Specification 5
2.3.1 Hardware Specification 5
2.3.2 Technical Specification 5
3. Base Installation **7**
3.1 Hardware Installation 7
3.1.1 System Requirements 7
3.1.2 Package Contents 7
3.1.3 Panel Function Descriptions 8
3.1.4 Installation Steps 9
3.2 Software Configuration 11
3.2.1 Network Configuration on PC 11
3.2.2 Quick Configuration 17
3.2.3 External Network Access 25
4. Web Interface Configuration **28**
4.1 System Configuration 29
4.1.1 Configuration Wizard 29
4.1.2 System Information 30
4.1.3 WAN Configuration 32
4.1.4 LAN1 & LAN2 Configuration 34
4.1.5 LAN3 & LAN4 Configuration 36
4.1.6 Wireless Configuration 39
4.2 User Authentication 45
4.2.1 Authentication Configuration 45
4.2.2 Black List Configuration 75
4.2.3 Policy Configuration 77
4.2.4 Guest User Configuration 81
4.2.5 Additional Configuration 82
4.3 Network Configuration 99
4.3.1 Network Address Translation 99
4.3.2 Privilege List 101

4.3.3 Monitor IP List....103
4.3.4 Walled Garden List....104
4.3.5 Proxy Server Properties....105
4.3.6 Dynamic DNS....106
4.4 Utilities....107
4.4.1 Change Password....107
4.4.2 Backup/Restore Setting....109
4.4.3 Firmware Upgrade....109
4.4.4 Restart....110
4.5 Status....111
4.5.1 System Status....111
4.5.2 Interface Status....113
4.5.3 Current Users....116
4.5.4 Traffic History....117
4.5.5 Notify Configuration....118
4.6 Help....119
5. Appendix A -- Console Interface....120
6. Appendix B -- Configuration on Authorize.Net....123
7. Appendix C -- Proxy Setting for Hotspot....127
8. Appendix D -- Proxy Setting for Enterprise....130
9. Appendix E -- Disclaimer for On-Demand Users....135

1. Before You Start

1.1 Preface

This manual is for Hotspot owners or administrators in enterprises to set up network environment using WAS-102R. It contains step by step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation.

1.2 Document Conventions

- For any caution or warning that requires special attention of readers, a highlight box with the eye-catching italic font is used as below:

Warning: *For security purposes, you should immediately change the Administrator's password.*

Indicates that clicking this button will return to the homepage of this section.

Indicates that clicking this button will return to the previous page.

Indicates that clicking this button will apply all of your settings.

Indicates that clicking this button will clear what you set before these settings are applied.

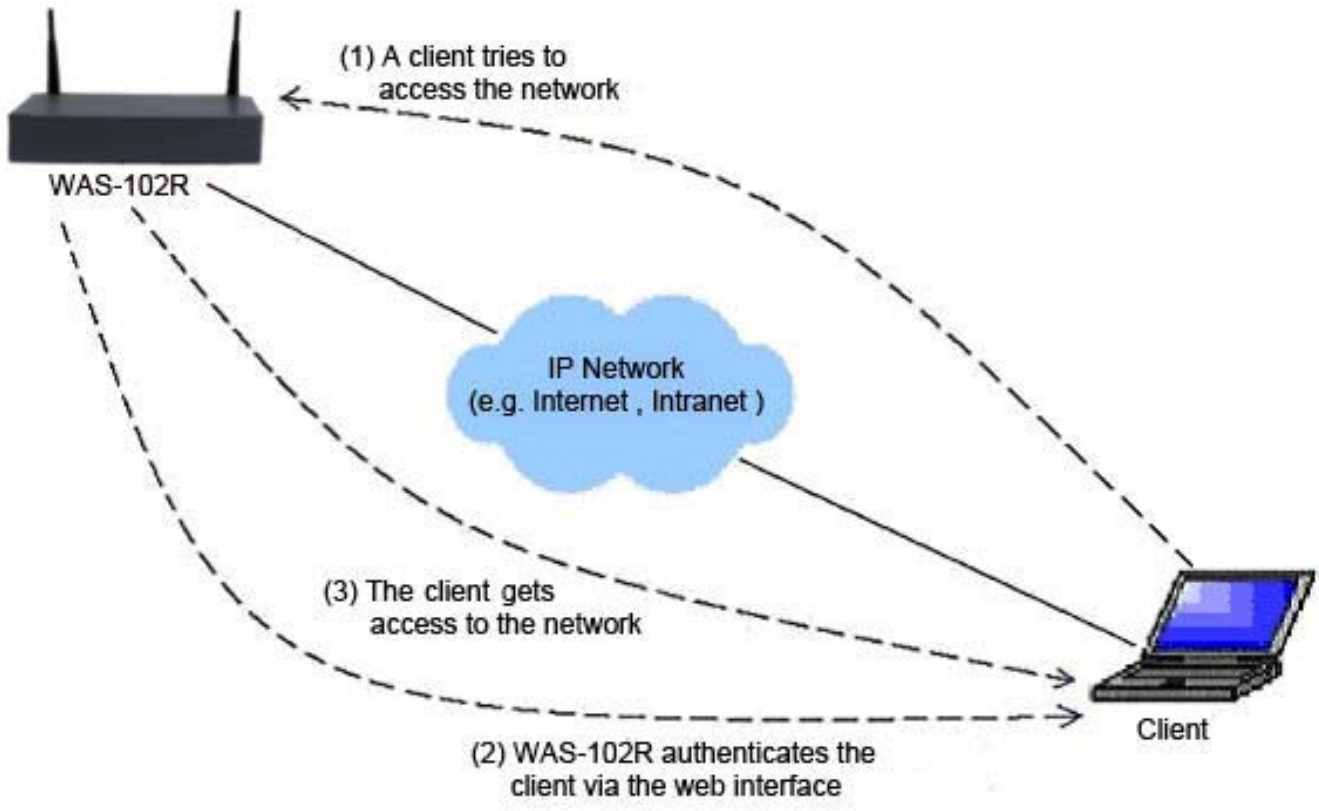
2. System Overview

2.1 Introduction of WAS-102R

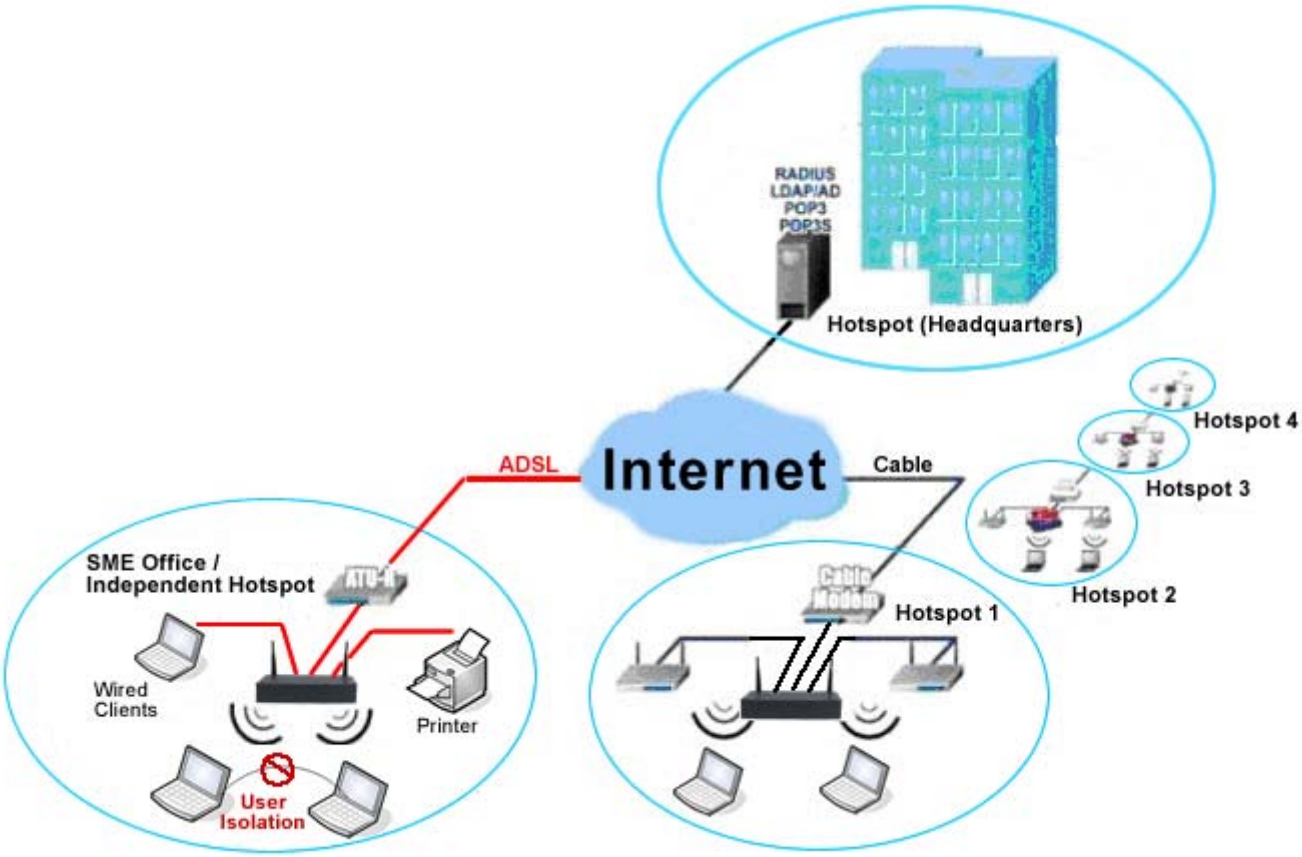
WAS-102R is an all-in-one product specially designed for small wireless network environment. It integrates **"Access Control"** and **"Wireless Network Access"** into one system to fulfill the needs in Hotspot environment. WAS-102R supports 802.11b and 802.11g dual wireless transmission modes and at the same time incorporates **"convenience," "efficiency,"** and **"friendliness"** for services.

2.2 System Concept

WAS-102R is specially designed for user authentication, authorization and management. The user account information is stored in the local database or a specified external databases server. The user authentication is processed via the SSL encrypted web interface. This interface is compatible to most desktop devices and palm computers. The following figure is an example of WAS-102R set to control a part of the company's intranet. The whole managed network includes the cable network users and the wireless network users.



The users located at the managed network will be unable to access the network resource without permission. When the browser of a user attempts to connect to a website, the WAS-102R will force the browser to redirect to the user login webpage. The user must enter the username and password for authentication. After the identity is authenticated successfully, the user will gain proper access right defined on the WAS-102R.



2.3 Specification

2.3.1 Hardware Specification

- Dimensions: 15.0cm(W) x4.0cm(H) x 23.0cm(L)
- Weight: 3 kg
- Power: DC12V/1A 5.5Φ
- Operating Temperature: 5-45°C
- 5 Fast Ethernet RJ 45 Connectors
- 1 Console Port
- Supports 10/100Mbps Full / Half Duplex Transfer Speed

2.3.2 Technical Specification

- **Standards**

  This system supports IEEE 802.1x, 802.11b and 802.11g

- **Networking**

  WAN interface supports Static IP, DHCP client, and PPPoE client

  Interface supports static IP

Supports NAT mode and router mode

Built-in DHCP server

Built-in NTP client

Supports Redirect of network data

Supports IPSec (ESP), PPTP and H.323 pass through (under NAT)

Customizable static routing table

Supports Virtual Server

Supports DMZ Server

Supports machine operation status monitoring and reporting system

- **Firewall**

  Provides Several DoS protection mechanisms

  Customizable packet filtering rules

  Customizable walled garden (free surfing area)

- **User Management**

  Supports up to 500 local users.

  Supports Local, POP3 (+SSL), RADIUS, and LDAP LAN1/LAN2 mechanisms

  Supports LAN1& LAN2 mechanisms simultaneously

  Can choose MAC address locking for built-in user database

  Can set the time for the user to log in to the system

  Can set the user's idle time

  Can specify the MAC addresses to enter the managed network without authentication

  Can specify the IP addresses to enter the managed network without authentication

  Supports the setting to pass or block all the connections when the WAN interface failed

  Supports web-based login

  Supports several friendly logout methods

  Supports RADIUS accounting protocol to generate the billing record on RADIUS server

- **Administration**

  Provides online status monitoring and history traffic

  Supports SSL encrypted web administration interface and user login interface

  Customizable user login & logout web interface

  Customizable redirect after users are successfully authenticated during login & logout

  Supports Console management interface

  Supports SSH remote administration interface

  Supports web-based administration interface

  Supports SNMP v2

  Supports user's bandwidth restriction

  Supports remote firmware upgrade

- **Accounting**

  Supports built-in user database and RADIUS accounting

3. Base Installation

3.1 Hardware Installation

3.1.1 System Requirements

- Standard 10/100BaseT including five network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

3.1.2 Package Contents

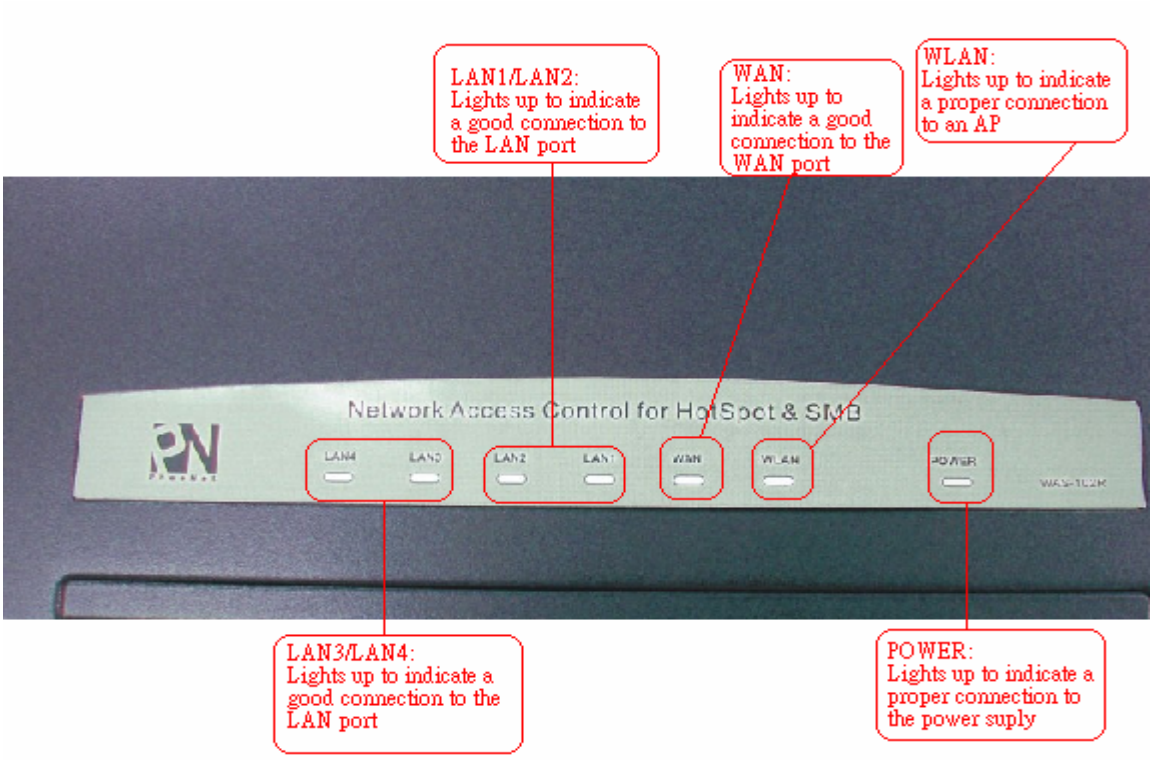
The standard package of WAS-102R includes:

- WAS-102R x 1
- CD-ROM x 1
- Quick Installation Guide x 1
- Power Adaptor (DC 12V) x 1
- Cross Over Ethernet Cable x 1
- Console Cable x 1
- 2dbi Omni-antenna x 2

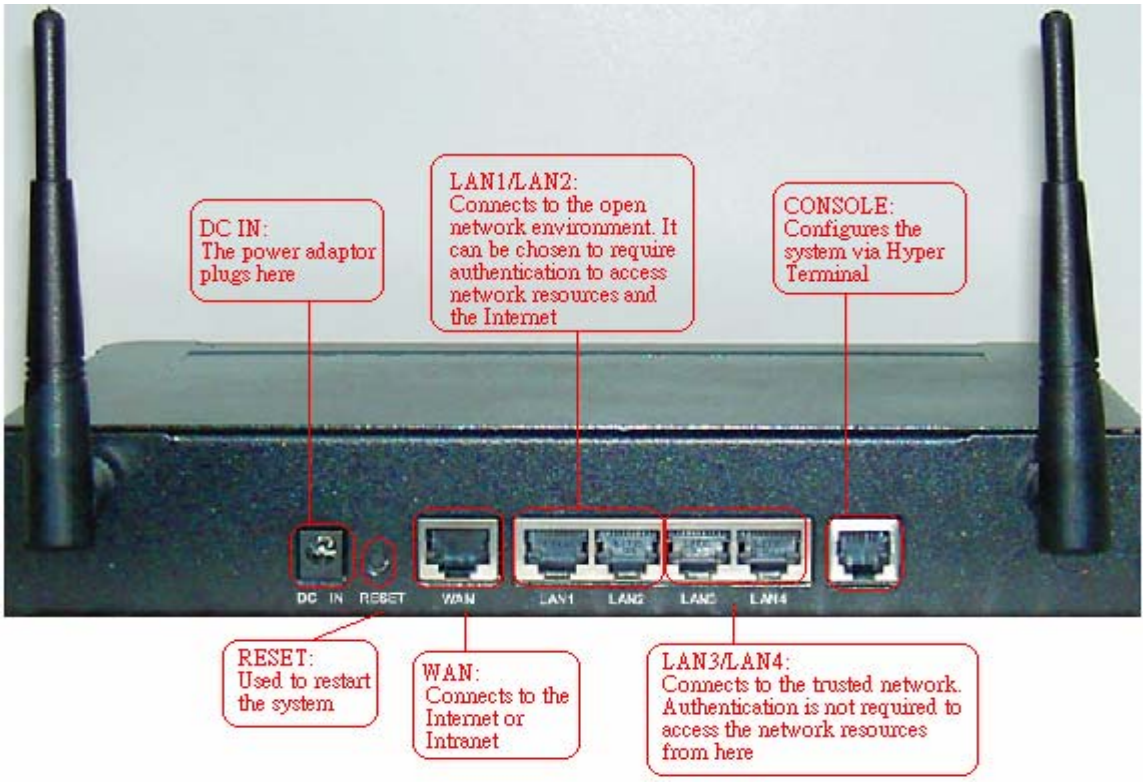
Warning: *It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.*

3.1.3 Panel Function Descriptions

Front Panel


LAN1/LAN2:
Lights up to indicate a good connection to the LAN port
WAN:
Lights up to indicate a good connection to the WAN port
WLAN:
Lights up to indicate a proper connection to an AP
Network Access Control for HotSpot & SMB
LAN4
LAN3
LAN2
LAN1
WAN
WLAN
POWER
LAN3/LAN4:
Lights up to indicate a good connection to the LAN port
POWER:
Lights up to indicate a proper connection to the power suply

Rear Panel



- **DC IN:** The power adaptor attaches here.
- **RESET:** Press this button to restart the system.
- **WAN:** The WAN port is used to connect to a network which is not managed by the WAS-102R system, and this port can be used to connect the ATU-Router of ADSL, the port of Cable Modem, or the Switch or Hub on the LAN of a company.
- **LAN1/LAN2:** The two LAN ports are connected to the managed network or WLAN. They can be selected to require or not require authentication to access network resources and Internet.
- **LAN3/LAN4:** The two LAN ports are connected to a trustful network where the users can always use the network resources without authentication. This port can be connected to a server such as File Server or a Database Server, etc.
- **Console:** The system can be configured via HyperTerminal. For example, if you need to set the Administrator's Password, you can connect a PC to this port as a Console Serial Port via a terminal connection program (such as the super terminal with the parameters of 9600, 8, N, 1, None flow control) to change the Administrator's Password.

3.1.4 Installation Steps

Please follow the following steps to install WAS-102R:

1. Connect the DC power adapter to the power connector socket on the rear panel. The Power LED should be on to indicate a proper connection.
2. Connect an Ethernet cable to the WAN Port on the rear panel. Connect the other end of the Ethernet cable to ADSL modem, cable modem or a switch/hub of the internal network. The LED of this WAN port should be on to indicate a proper connection.
3. Connect an Ethernet cable to the LAN1/LAN2 Port on the rear panel. Connect the other end of the Ethernet cable to an AP or switch. The LED of LAN1/LAN2 should be on to indicate a proper connection. (Note: Authentication is required for the users to access the network via these LAN Ports. The LAN port with authentication function is referred to as ***Public LAN***.)
4. Connect an Ethernet cable to the LAN3/LAN4 Port on the rear panel. Connect the other end of the Ethernet cable to a client's PC. The LED of LAN3/LAN4 should be on to indicate a proper connection. (Note: No authentication is required for the users to access the network via these LAN Ports. The LAN port without authentication function is referred to as ***Private LAN*** and the administrator can enter the administrative user interface to perform configurations via Private LAN.)

Attention: *WAS-102R supports Auto Sensing MDI/MDIX. You may also use either straight through or cross over cable to connect the Ethernet Port.*

After the hardware of WAS-102R is installed completely, the system is ready to be configured in the following sections. The manual will guide you step by step to set up the system using a single WAS-102R to manage the network.

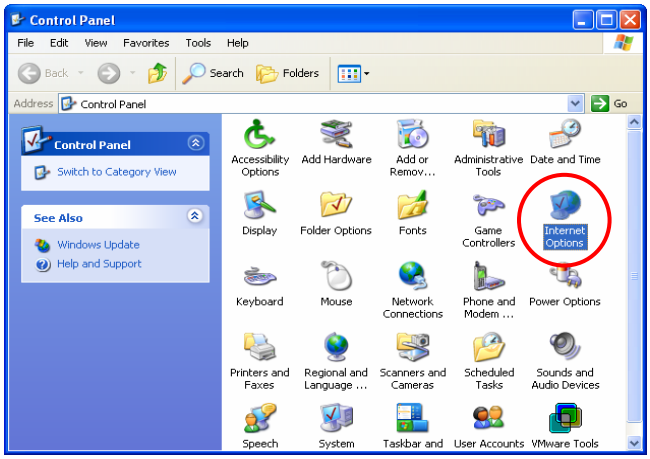
3.2 Software Configuration

3.2.1 Network Configuration on PC

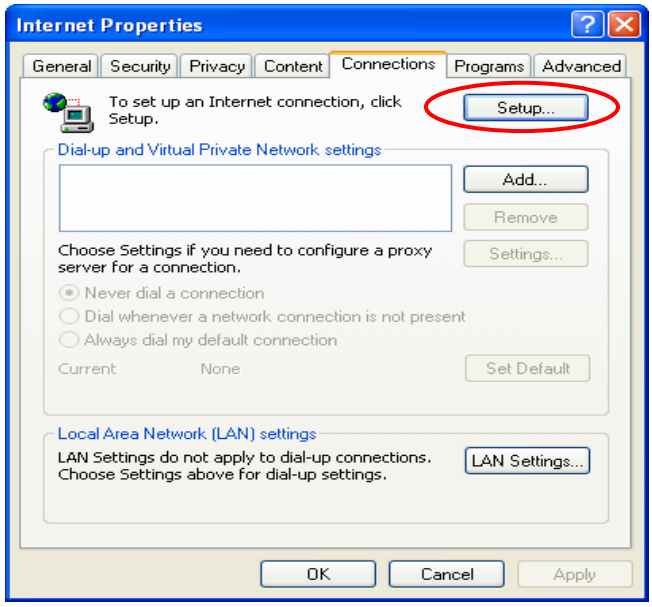
After WAS-102R is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**
  - ◆ **Windows XP**

1. Choose **Start** > **Control Panel** > **Internet Option**.



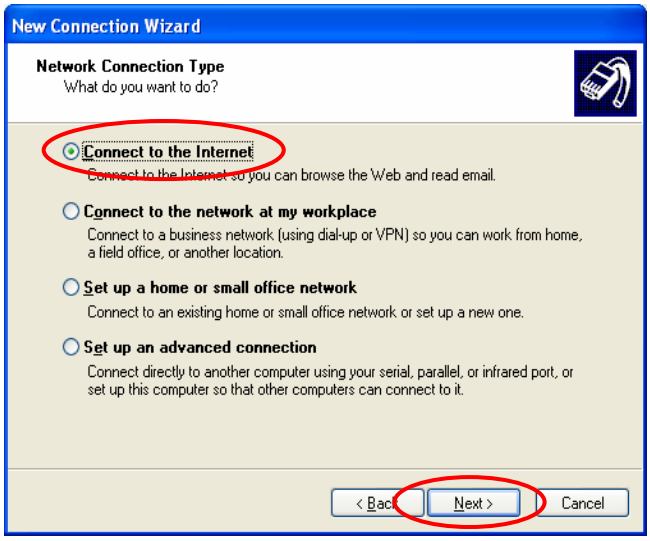
2. Choose the **"Connections"** label, and then click ***Setup***.


Internet Properties
General Security Privacy Content Connections Programs Advanced
To set up an Internet connection, click Setup.
Setup...
Dial-up and Virtual Private Network settings
Add...
Remove
Choose Settings if you need to configure a proxy server for a connection.
Settings...
Never dial a connection
Dial whenever a network connection is not present
Always dial my default connection
Current None
Set Default
Local Area Network (LAN) settings
LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.
LAN Settings...
OK
Cancel
Apply

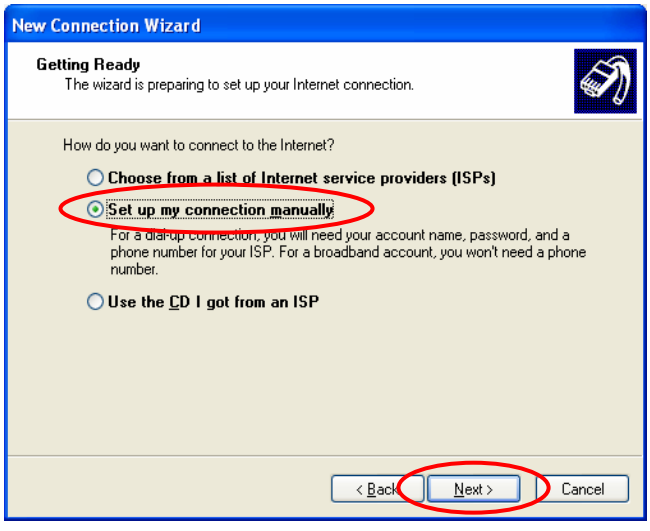
3. Click ***Next*** when **Welcome to the New Connection Wizard** screen appears.

New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
• Connect to the Internet.
• Connect to a private network, such as your workplace network.
• Set up a home or small office network.
To continue, click Next.
< Back
Next >
Cancel

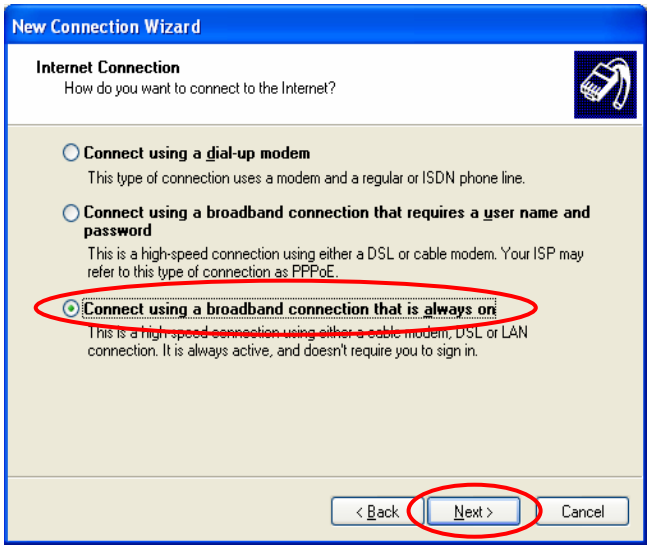
4. Choose **"Connect to the Internet"** and then click ***Next***.


New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

5. Choose **"Set up my connection manually"** and then click ***Next***.


New Connection Wizard
Getting Ready
The wizard is preparing to set up your Internet connection.
How do you want to connect to the Internet?
Choose from a list of Internet service providers (ISPs)
Set up my connection manually
For a dial-up connection, you will need your account name, password, and a phone number for your ISP. For a broadband account, you won't need a phone number.
Use the CD I got from an ISP
< Back
Next >
Cancel

6. Choose **"Connect using a broadband connection that is always on"** and then click ***Next***.


New Connection Wizard
Internet Connection
How do you want to connect to the Internet?
Connect using a dial-up modem
This type of connection uses a modem and a regular or ISDN phone line.
Connect using a broadband connection that requires a user name and password
This is a high-speed connection using either a DSL or cable modem. Your ISP may refer to this type of connection as PPPoE.
Connect using a broadband connection that is always on
This is a high-speed connection using either a cable modem, DSL or LAN connection. It is always active, and doesn't require you to sign in.
< Back
Next >
Cancel

7. Finally, click ***Finish*** to exit the **Connection Wizard**. Now, the setup is complete.

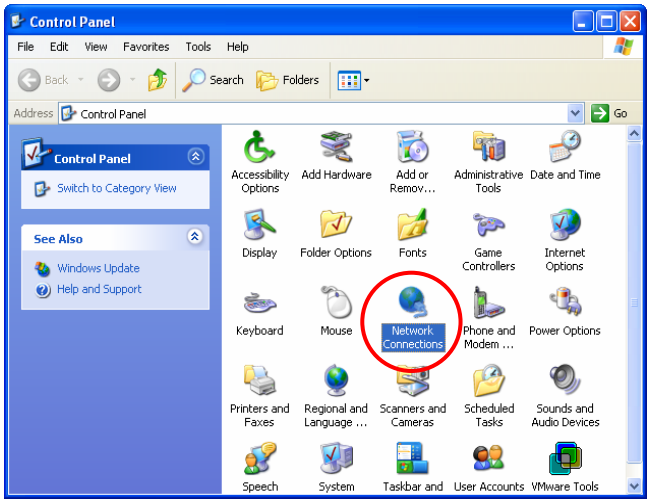
New Connection Wizard
Completing the New Connection Wizard
Your broadband connection should already be configured and ready to use. If your connection is not working properly, click the following link.
Learn more about broadband connections.
To close this wizard, click Finish.
< Back
Finish
Cancel

- **TCP/IP Network Setup**

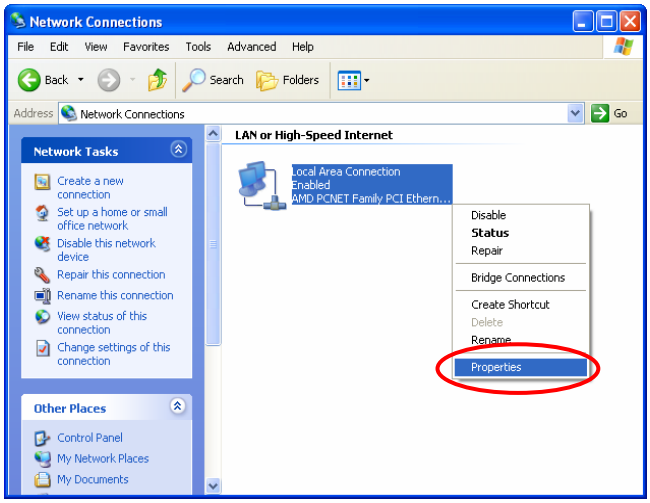
  If the operating system of the PC in use is Windows 95/98/ME/2000/XP, keep the default settings without any change to directly start/restart the system. With the factory default settings, during the process of starting the system, WAS-102R with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called **"Obtain an IP address automatically"**. If checking the TCP/IP setup or using the static IP in the LAN1/LAN2 or LAN3/LAN4 section is desired, please follow these steps:

◆ **Check the TCP/IP Setup of Window XP**

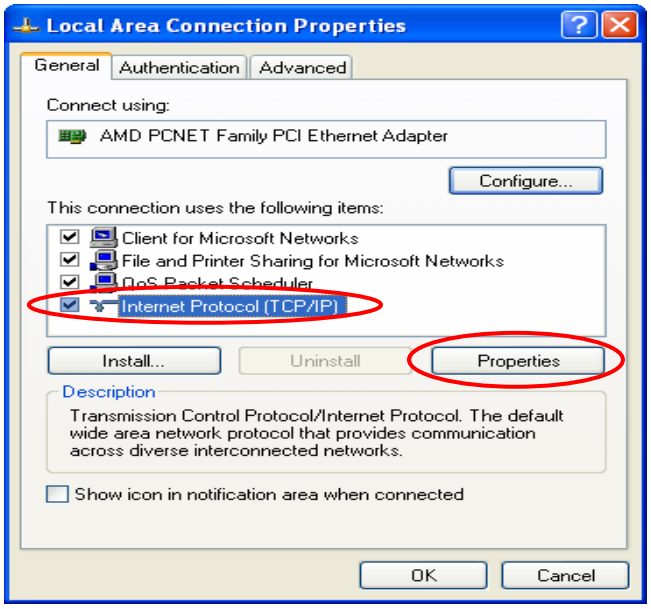
1. Select **Start > Control Panel > Network Connection**.



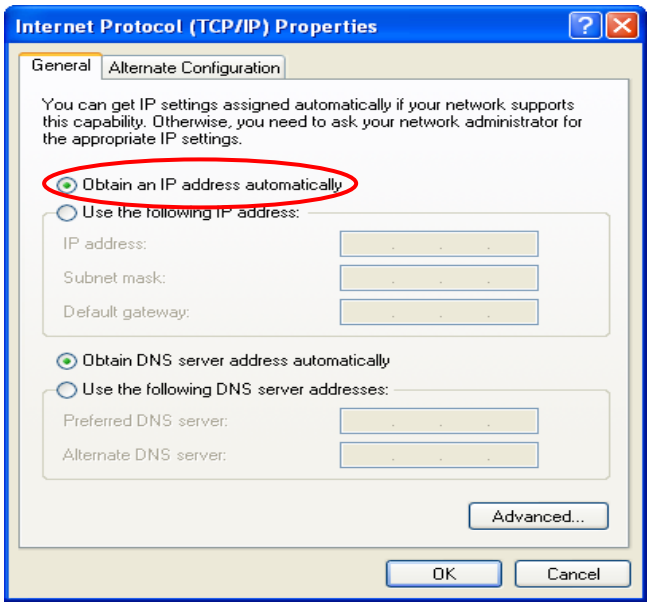
2. Click the right button of the mouse on the **"Local Area Connection"** icon and select **"Properties"**



3. Select **"General"** label and choose **"Internet Protocol (TCP/IP)"** and then click ***Properties***. Now, choose to use **DHCP** or **specific IP address**, please proceed to the following steps.



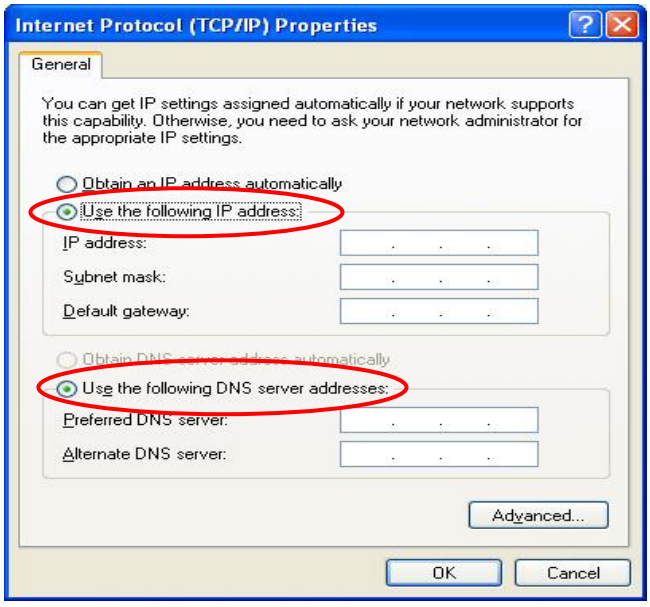
4-1. **Using DHCP:** If want to use DHCP, please choose **"Obtain an IP address automatically"** and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WAS-102R.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

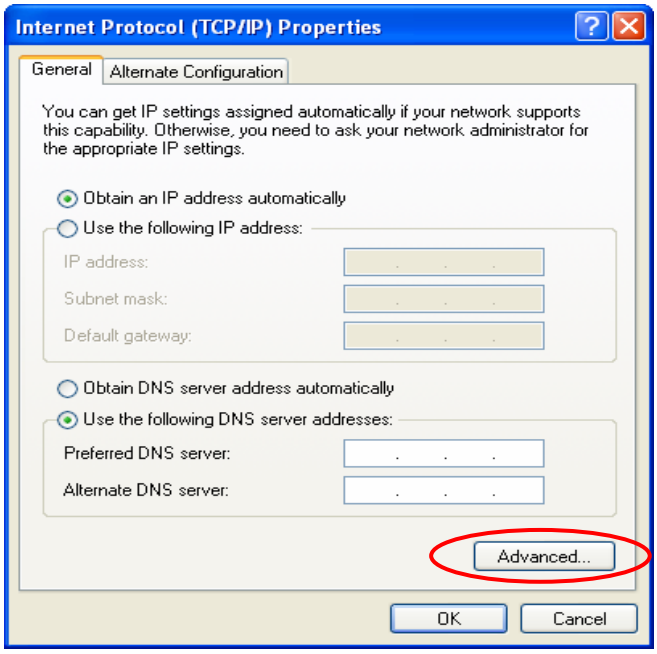
4-2. **Using Specific IP Address:** If using specific IP address is desired, ask the network administrator for the information of the WAS-102R: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

Caution: *If your PC has been set up completed, please inform the network administrator before proceeding to the following steps.*

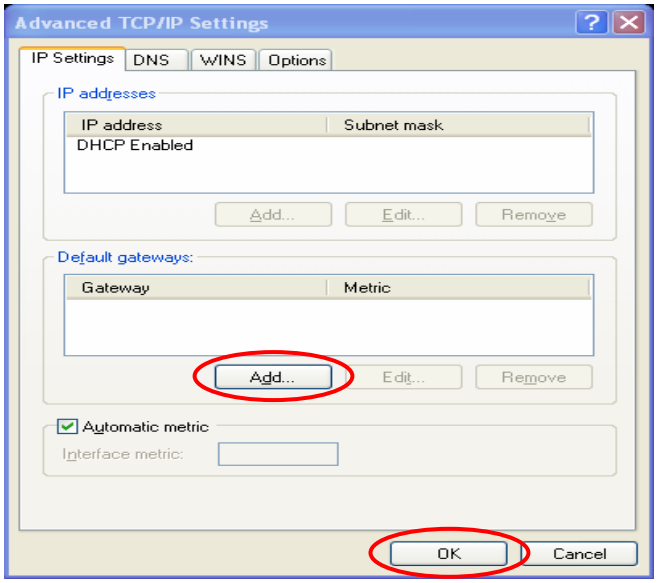
- Please choose **"Use the following IP address"** and enter the information given from the network administrator in **"IP address"** and **"Subnet mask"** If the DNS Server column is blank, please choose **"Using the following DNS server addresses"** and then enter the DNS address or the DNS address provided by ISP and then click ***OK***.

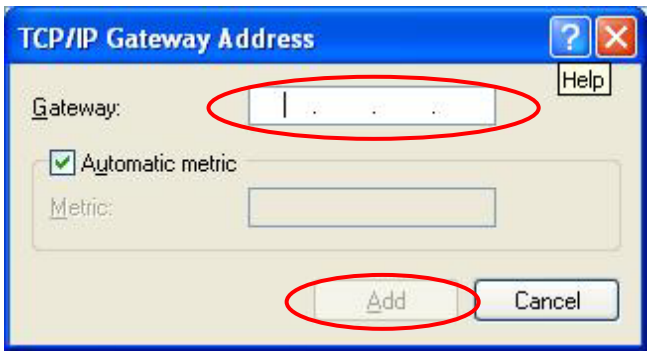

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

- Then, click ***Advanced*** in the window of **"Internet Protocol (TCP/IP)"**.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

- Choose the **"IP Settings"** label and click **"Add"** below the **"Default Gateways"** column and the **"TCP/IP Gateway Address"** window will appear. Enter the gateway address of WAS-102R in the **"Gateway"** of **"TCP/IP Gateway Address"** window, and then click ***Add***. After back to the **"IP Settings"** label, click ***OK*** to finish.





3.2.2 Quick Configuration

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 7 steps providing a simple and easy way to guide you through the setup of WAS-102R. Follow the procedures and instructions given by the Wizard to enter the required information step by step. After saving and restarting WAS-102R, it is ready to use. There will be **7** steps as listed below:

1. Change Admin's Password
2. Choose System's Time Zone
3. Set System Information
4. Select the Connection Type for WAN Port
5. Set Authentication Methods
6. Set Wireless – Access Point Connection
7. Save and Restart WAS-102R

Please follow the following steps to complete the quick configuration

1. Use the network cable of the 10/100BaseT to connect PC to the LAN3/LAN4 port, and then start a browser (such as Microsoft IE). Next, enter the gateway address for that port, the default is https://192.168.2.254. In the opened webpage, a login screen will appear. Enter ***"admin"***, the default username, and ***"admin"***, the default password, in the User Name and Password columns. Click ***Enter*** to log in.

Caution: *If you can't get the login screen, you may have incorrectly set your PC to obtain an IP address automatically from authentication LAN port or the IP address used does not have the same subnet as the URL. Please use default IP address such as 192.168.2.xx in your network and then try it again.*

You can log in as **admin**, **manager** or **operator**. The default username and password as follows.

Admin: The administrator can access all area of the WAS-102R.

User Name: **admin**

Password: **admin**

Manager: The manager only can access the area under ***User Authentication*** to manager the user account, but no permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

Password: **manager**

Operator: The operator only can access the area of ***Create On-demand User*** to create and print out the new on-demand user accounts.

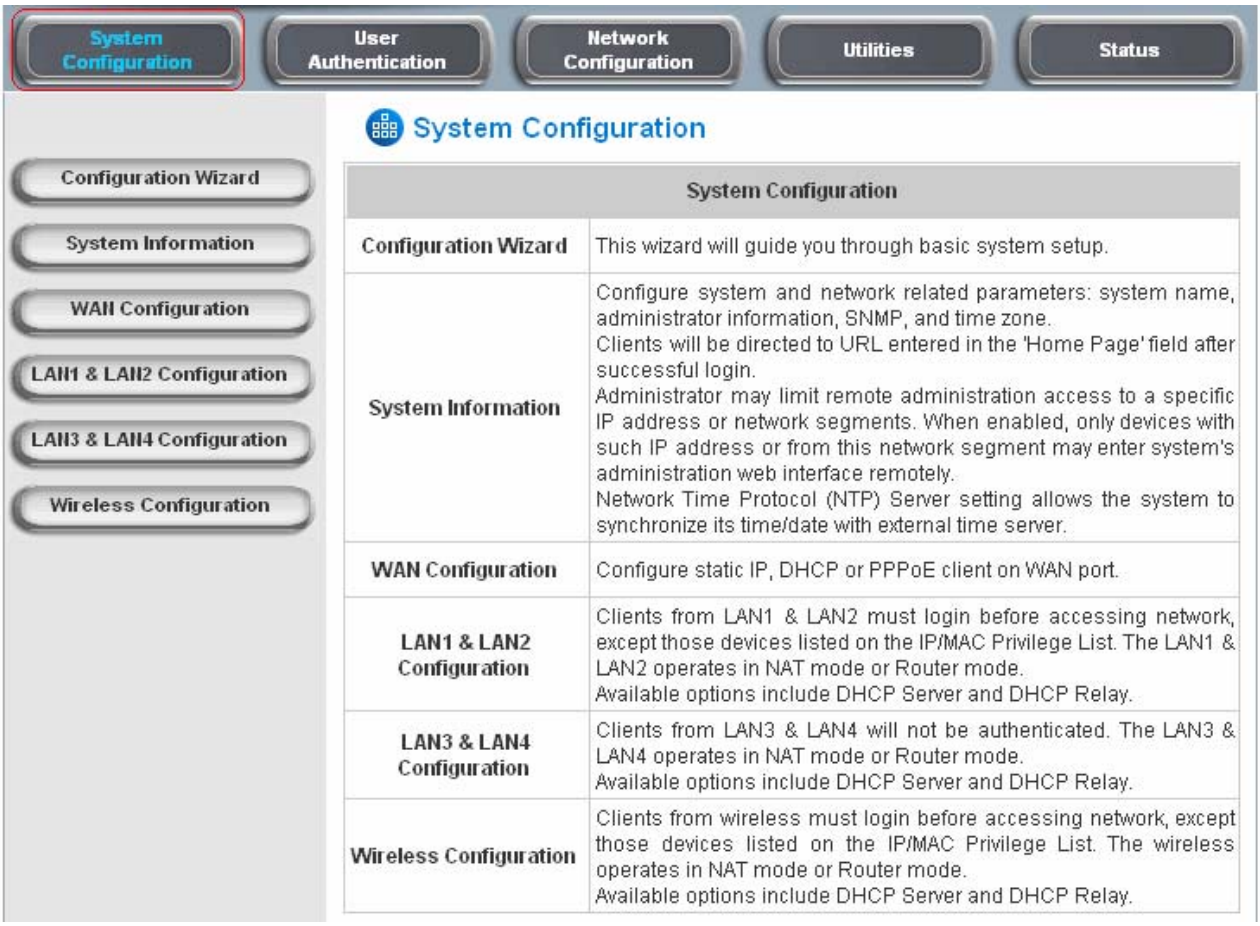
User Name: **operator**

Password: **operator**

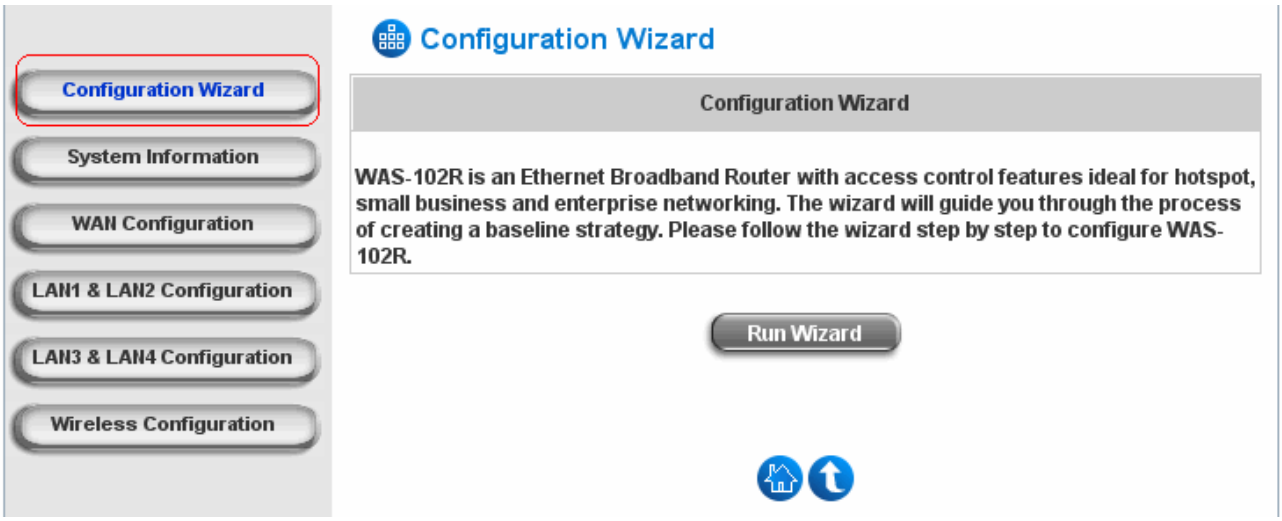
2. After successfully logging into WAS-102R, enter the web management interface and see the welcome screen. There is a ***Logout*** button on the upper right corner to log out the system when finished.

System Configuration
User Authentication
Network Configuration
Utilities
Status
Welcome to System Administration
This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.
Functions are separated into 5 main categories:
System Configuration , User Authentication , Network Configuration , Utilities and Status.

3. Then, run the configuration wizard to complete the configuration. Click ***System Configuration*** to the **System Configuration** homepage.


System Configuration
User Authentication
Network Configuration
Utilities
Status
Configuration Wizard
System Information
WAN Configuration
LAN1 & LAN2 Configuration
LAN3 & LAN4 Configuration
Wireless Configuration
System Configuration
System Configuration
Configuration Wizard
This wizard will guide you through basic system setup.
System Information
Configure system and network related parameters: system name, administrator information, SNMP, and time zone.
Clients will be directed to URL entered in the 'Home Page' field after successful login.
Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely.
Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
WAN Configuration
Configure static IP, DHCP or PPPoE client on WAN port.
LAN1 & LAN2 Configuration
Clients from LAN1 & LAN2 must login before accessing network, except those devices listed on the IP/MAC Privilege List. The LAN1 & LAN2 operates in NAT mode or Router mode.
Available options include DHCP Server and DHCP Relay.
LAN3 & LAN4 Configuration
Clients from LAN3 & LAN4 will not be authenticated. The LAN3 & LAN4 operates in NAT mode or Router mode.
Available options include DHCP Server and DHCP Relay.
Wireless Configuration
Clients from wireless must login before accessing network, except those devices listed on the IP/MAC Privilege List. The wireless operates in NAT mode or Router mode.
Available options include DHCP Server and DHCP Relay.

4. Click the ***System Configuration*** from the top menu and the homepage of **System Configuration** will appear. Then, click on ***Configuration Wizard*** and click the ***Run Wizard*** button to start the wizard.


Configuration Wizard
System Information
WAN Configuration
LAN1 & LAN2 Configuration
LAN3 & LAN4 Configuration
Wireless Configuration
Configuration Wizard
Configuration Wizard
WAS-102R is an Ethernet Broadband Router with access control features ideal for hotspot, small business and enterprise networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure WAS-102R.
Run Wizard

5. **Configuration Wizard**

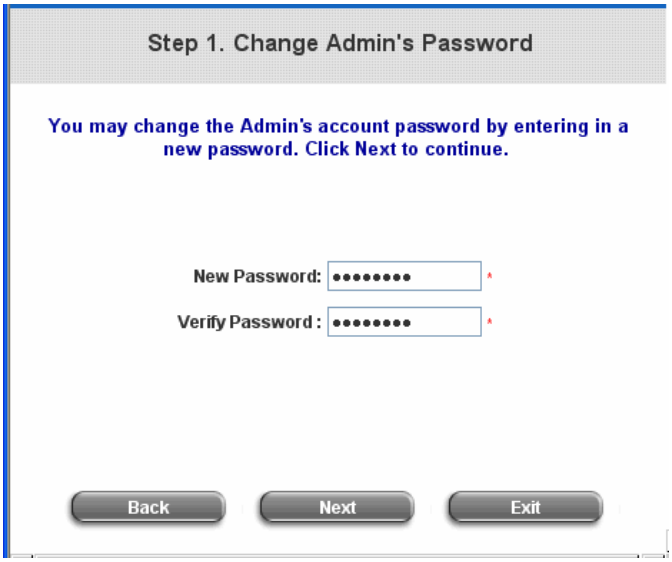
A welcome screen that briefly introduces the 7 steps will appear. Click ***Next*** to begin.

Configuration Wizard
Welcome to the Setup Wizard. The wizard will guide you through these 7 quick steps. Begin by clicking on Next.
Step 1. Change Admin's Password
Step 2. Choose System's Time Zone
Step 3. Set System Information
Step 4. Select the Connection Type for WAN Port
Step 5. Set Authentication Methods
Step 6. Set Wireless-Access Point Connection
Step 7. Save and Restart WAS-102R
Next
Exit

- **Step 1. Change Admin's Password**

  Enter a new password for the admin account and retype it in the verify password field (twenty-character maximum and no spaces).

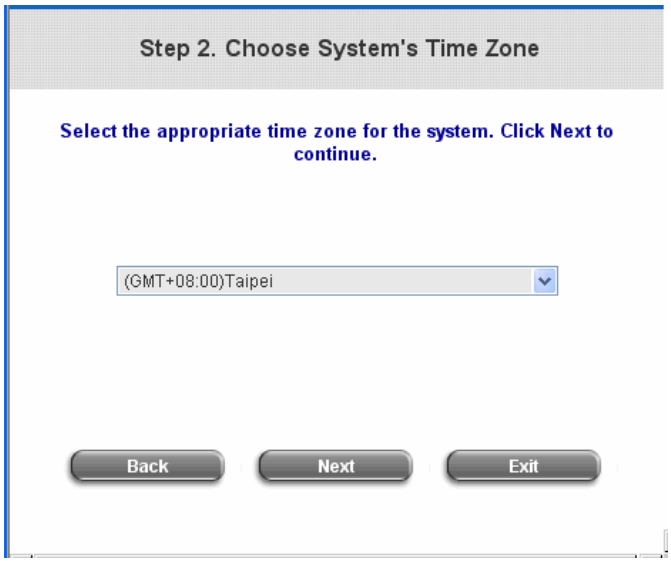
  Click ***Next*** to continue.


Step 1. Change Admin's Password
You may change the Admin's account password by entering in a new password. Click Next to continue.
New Password:
Verify Password :
Back
Next
Exit

- **Step 2.: Choose System's Time Zone**

  Select a proper time zone via the drop-down menu.

  Click ***Next*** to continue.



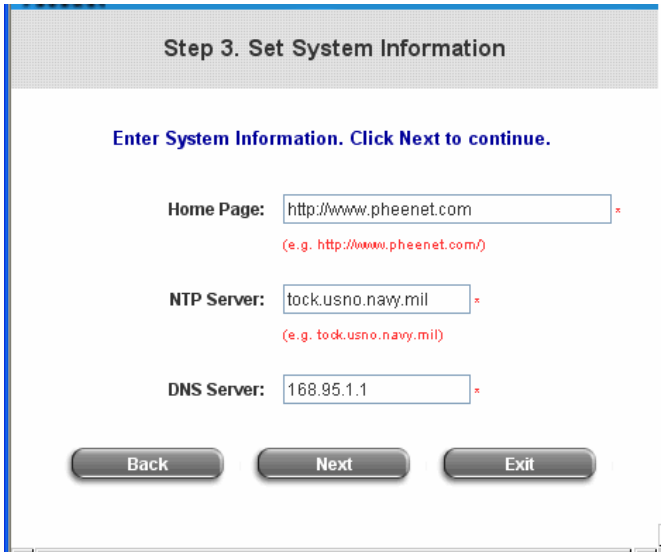
- **Step 3.: Set System Information**

  Home Page: Enter the URL to where the users should be directed when they are successfully authenticated.

  NTP Server: Enter the URL of external time server for WAS-102R time synchronization or use the default.

  DNS Server: Enter a DNS Server provided by the ISP (Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.

  Click ***Next*** to continue.



- **Step 4. Select the Connection Type for WAN Port**

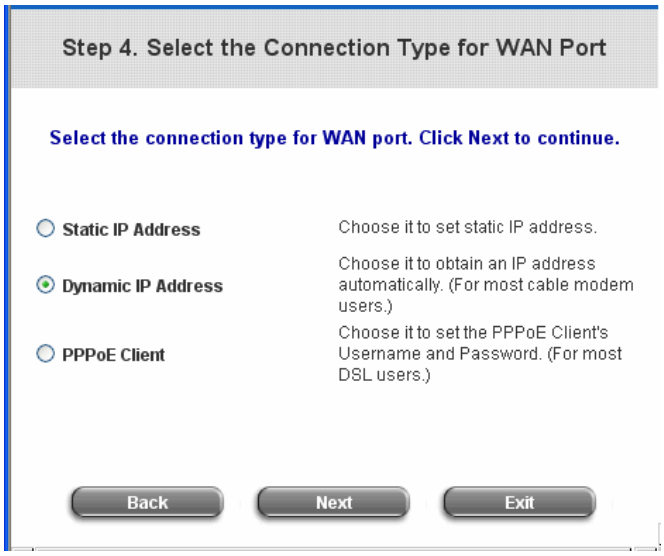
  Three are three types of WAN port to select: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**.

  Select a proper Internet connection type and click ***Next*** to continue.

  - **Dynamic IP Address**

    If this option is selected, an appropriate IP address and related information will automatically be assigned.

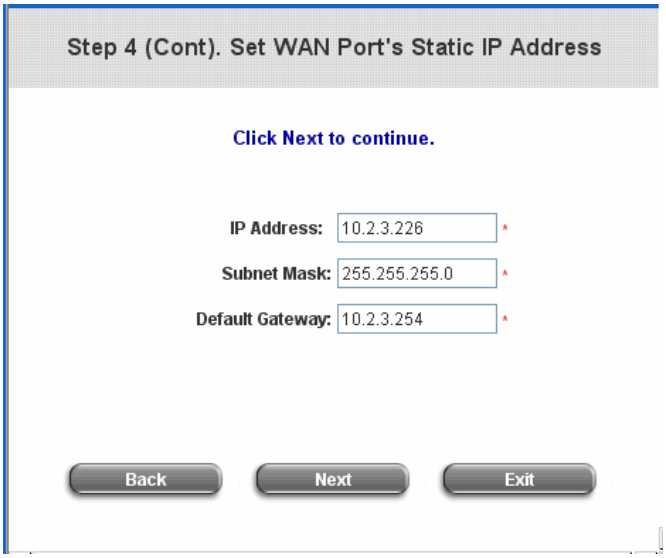
    Click ***Next*** to continue.


Step 4. Select the Connection Type for WAN Port
Select the connection type for WAN port. Click Next to continue.
Static IP Address
Choose it to set static IP address.
Dynamic IP Address
Choose it to obtain an IP address automatically. (For most cable modem users.)
PPPoE Client
Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)
Back
Next
Exit

  - **Static IP Address: Set WAN Port's Static IP Address**

    Enter the **"IP Address"**, **"Subnet Mask"** and **"Default Gateway"** provided by the ISP.

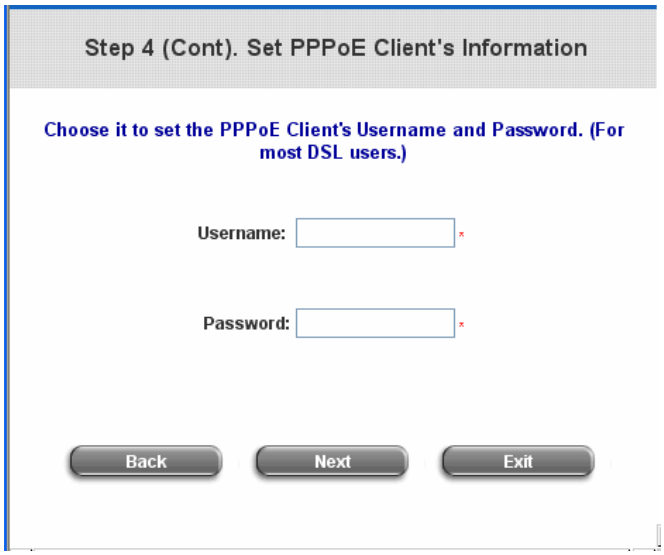
    Click ***Next*** to continue.



➢ **PPPoE Client: Set PPPoE Client's Information**

Enter the **"Username"** and **"Password"** provided by the ISP.

Click ***Next*** to continue.

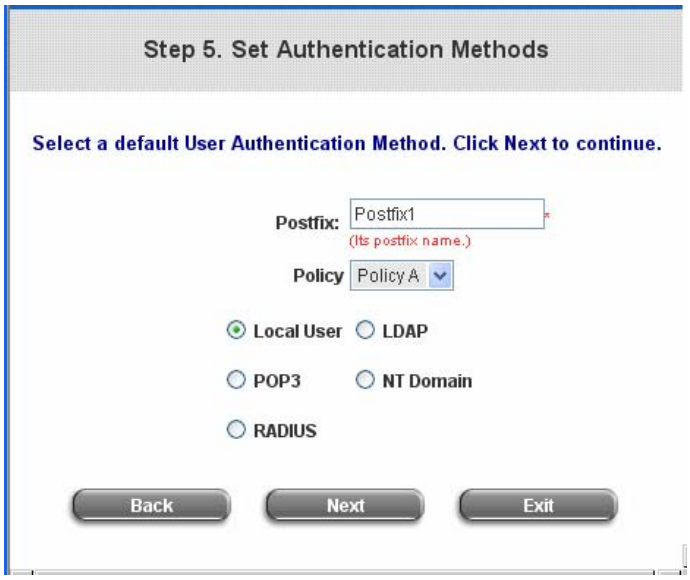


- **Step 5. Set Authentication Methods**

➢ Set the user's information in advance.

Enter an easily identified name as the postfix name in the ***Policy Name*** field (e.g. Local), select a policy to (or use the default value), and choose an authentication method.

Click ***Next*** to continue.



➢ **Local User: Add User**

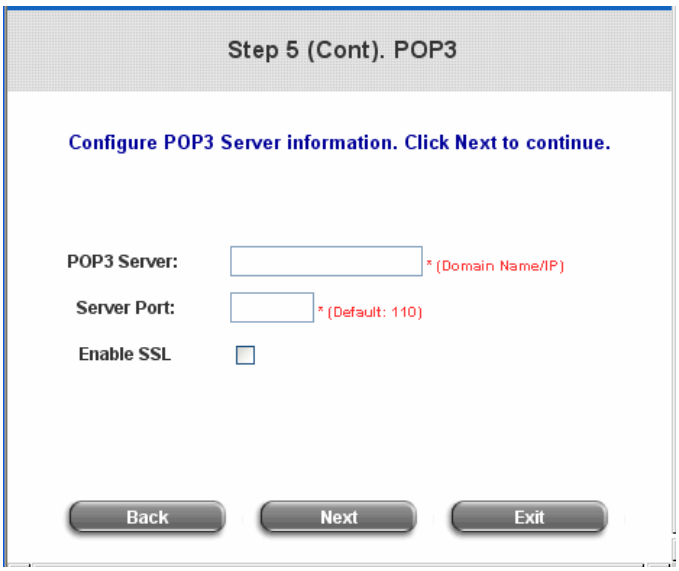
A new user can be added to the local user data base. To want to add a user here, enter the ***Username*** (e.g. test), ***Password*** (e.g. test), ***MAC*** (optional) and assign it a policy (or use the default). Upon completing a user adding, more users can be added to this authentication method by clicking the ***ADD*** bottom.

Click ***Next*** to continue.

POP3 User: POP3

Enter IP/Domain Name and server port of the POP3 server provided by the ISP, and then choose enable SSL or not.

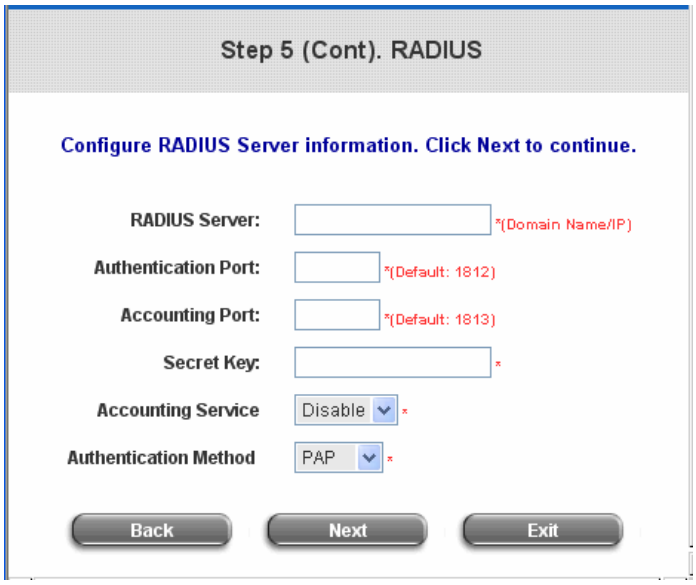
Click ***Next*** to continue.



- **RADIUS User: RADIUS**

  Enter RADIUS server IP/Domain Name, authentication port, accounting port and secret key. Then choose to enable accounting service or not, and choose the desired authentication method.

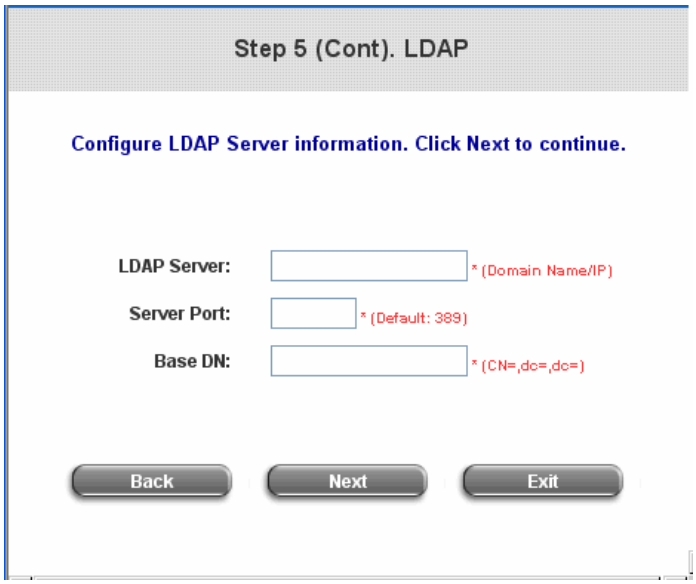
  Click ***Next*** to continue.



- **LDAP User: LDAP**

  Add a new user to the LDAP user data base if desired. Enter the **"LDAP Server"**, **"Server Port"**, and **"Base DN"**.

  Click **Next** to continue.

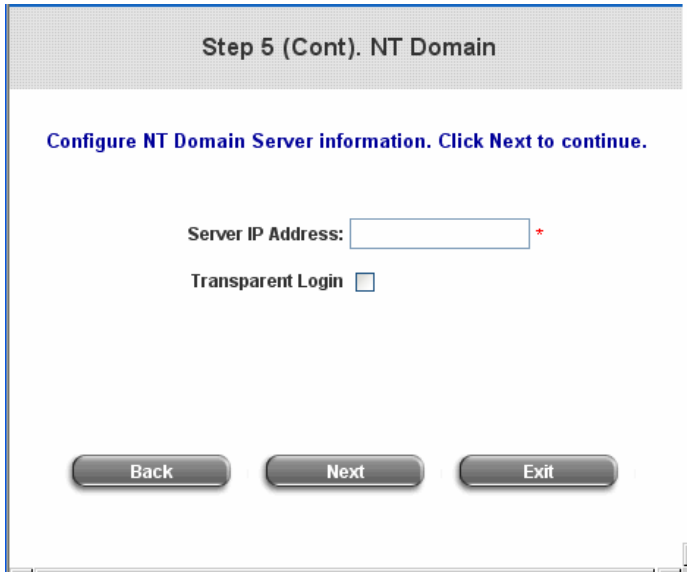


➢ **NT Domain User: NT Domain**

When NT Domain User is selected, enter the information for **"Server IP Address"**, and choose to enable/disable **"Transparent Login"**.

If "Transparent Login" is enabled, users are logged in WAS-102R's NT Domain active directory and authenticated automatically when they log into their Windows OS domain.

Click ***Next*** to continue.



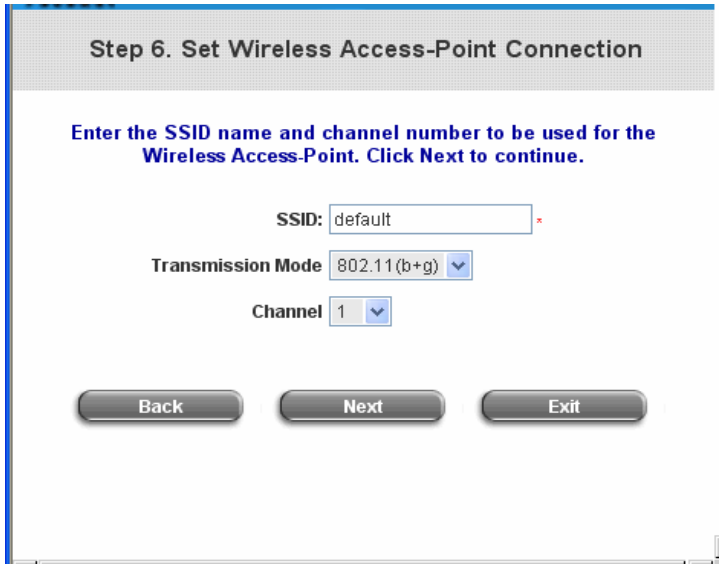
- **Step 6. Set Wireless – Access Point Connection**

SSID: Enter a SSID (up to 32 characters) for system. **SSID** (**S**ervice **S**et **Id**entifier) is a unique identifier used for the wireless users' devices to get associated with WAS-102R.

Transmission Mode: WAS-102R supports two transmission modes, **802.11b** and **802.11 (b+g)**. Select the appropriate transmission mode to work with the wireless clients in the network.

Channel: Select a channel from the **"Channel"** field for WAS-102R to function properly. ***(Note: the available channels depend upon the region. For instance, Channel 1~11 are available in Taiwan, and Channel 1-13 are available in Europe).***

Click ***Next*** to continue.

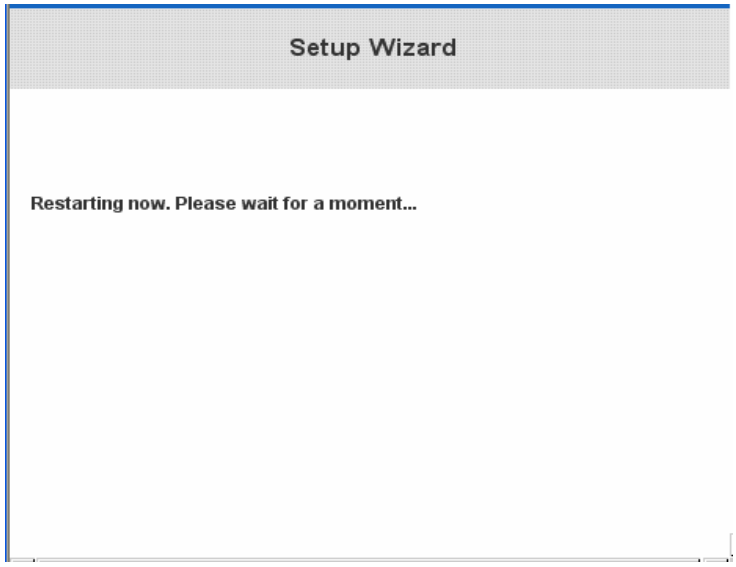

Step 6. Set Wireless Access-Point Connection
Enter the SSID name and channel number to be used for the Wireless Access-Point. Click Next to continue.
SSID: default
Transmission Mode 802.11(b+g)
Channel 1
Back
Next
Exit

- **Step 7. Save and Restart WAS-102R**

Click ***Restart*** to save the current settings and restart WAS-102R. The Setup Wizard is now completed.

Step 7. Save and Restart WAS-102R
The Setup Wizard has completed. Click on Back to modify changes or mistakes. Click Restart to save the current settings and reboot.
Back
Restart
Exit

- **Setup Wizard.** During WAS-102R restart, a **"Restarting now. Please wait for a while."** message will appear on the screen. Please do not interrupt WAS-102R until the message has disappeared. This indicates that a complete and successful restart process has finished.



Caution: *During every step of the wizard, if you wish to go back to modify the settings, please click the* ***Back*** *button to go back to the previous step.*

3.2.3 External Network Access

If all the steps are set properly, WAS-102R can be further connected to the managed network to experience the controlled network access environment. Firstly, connect an end-user device to the network at WAS-102R's LAN1/LAN2 and set to obtain an IP address automatically. After the network address is obtained at the user end, open an Internet browser and link to any website. Then, the default logon webpage will appear in the Internet browser.

1. First, connect a user-end device to LAN1/LAN2 port of the WAS-102R, and set the dynamical access network. After the user end obtains the network address, please open an Internet browser and the default login webpage will appear on the Internet browser.
   Key in the username and password created in the local user account or the on-demand user account in the interface and then click ***Submit*** button. Here, we key in the local user account (e.g. ***test@Local*** for the username and ***test*** for the password) to connect the network.

2. Login page appearing means WAS-102R has been installed and configured successfully. Now, the user can browse the network or surf the Internet!

3. If the screen shows **"Sorry, this feature is available for on-demand user only"**, the **"Remaining"** button has been clicked. This button is only for on-demand users. For users other than on-demand users, please click the ***Submit*** button.

4. An on-demand user can enter the username and password in the **"User Login Page"** and click the ***Remaining*** button to view the remaining time the account.

5. When an on-demand user logs in successfully, the following **Login Successfully** screen will appear. There is an extra line showing **"Remaining usage"** and a **"Redeem"** button.

- **Remaining usage:** Show the rest of use time that the on-demand user can surf Internet.
- **Redeem:** When the remaining time or data size is insufficient, the user has to pay for adding credit at the counter, and then, the user will get a new username and password. After clicking the ***Redeem*** button,a login screen will appear. Please enter the new username and password obtained and click ***Redeem*** button. The total available use time and data size after adding credit will show up.

Caution: *The maximum session time/data transfer is 24305 days/9,999,999 Mbyte. If the redeem amount exceeds this number, the system will automatically reject the redeem process.*

4. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the functions of WAS-102R.

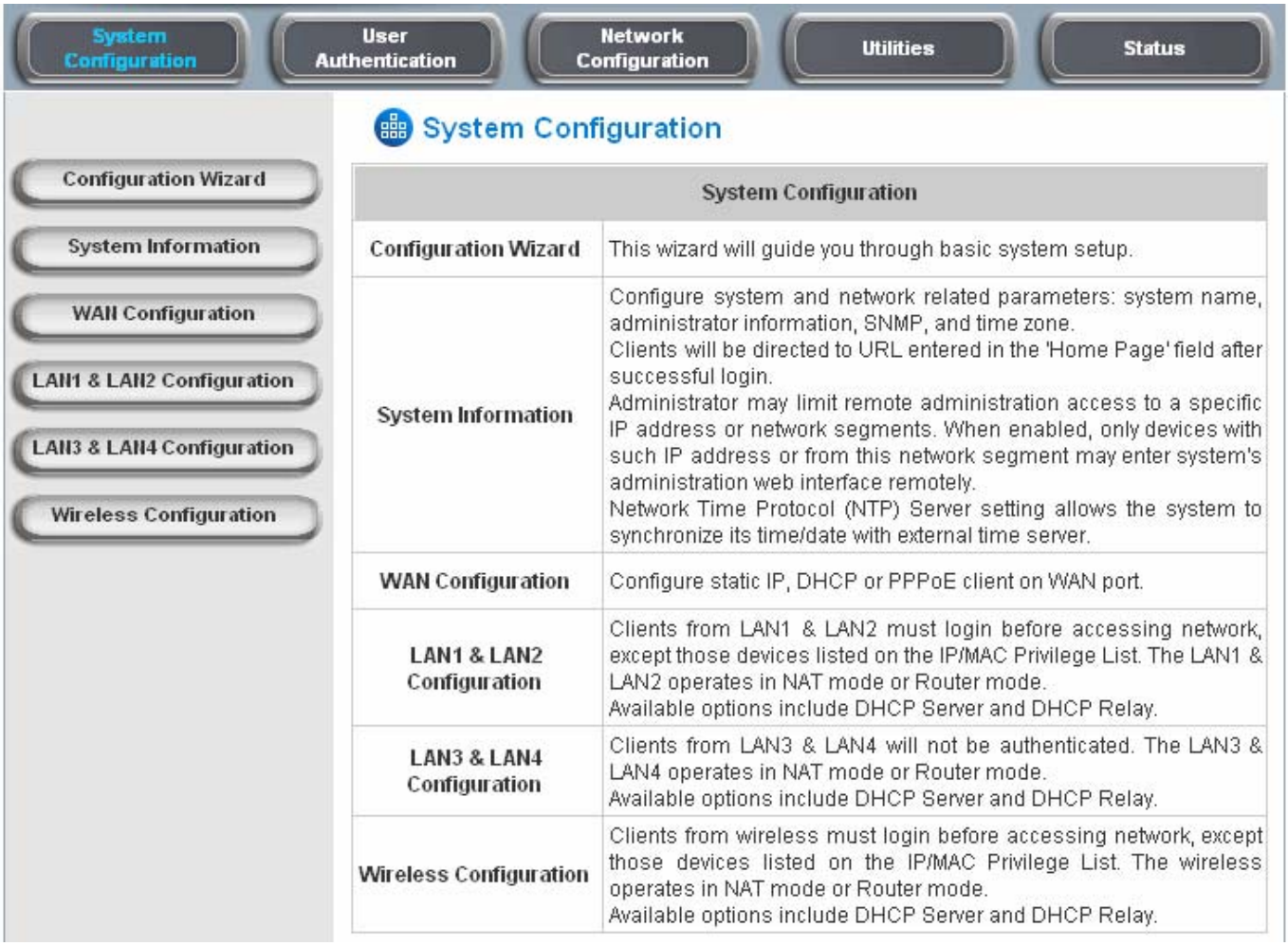
System Configuration
User Authentication
Network Configuration
Utilities
Status
Welcome to System Administration
This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.
Functions are separated into 5 main categories:
System Configuration , User Authentication , Network Configuration , Utilities and Status.

OPTION	System Configuration	User Authentication	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	Network Address Translation	Change Password	System Status
	System Information	Black List Configuration	Privilege List	Backup/Restore Strategy	Interface Status
	WAN Configuration	Policy Configuration	Monitor IP List	Firmware Upgrade	Current Users
	LAN1 & LAN2 Configuration	Guest User Configuration	Walled Garden List	Restart	Traffic History
	LAN3 & LAN4 Configuration	Additional Configuration	Proxy Server Properties		Notify Configuration
	Wireless Configuration		Dynamic DNS		

Caution: *After finishing the configuration of the settings, please click* ***Apply*** *and pay attention to see if a restart message appears on the screen. If such message appears, system must be restarted to allow the settings to take effect. All on-line users will be disconnected during restart.*

4.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN Configuration**, **LAN1 & LAN2 Configuration**, **LAN3 & LAN4 Configuration** and **Wireless Configuration**.


System Configuration
User Authentication
Network Configuration
Utilities
Status
Configuration Wizard
System Information
WAN Configuration
LAN1 & LAN2 Configuration
LAN3 & LAN4 Configuration
Wireless Configuration
System Configuration
System Configuration
Configuration Wizard
This wizard will guide you through basic system setup.
System Information
Configure system and network related parameters: system name, administrator information, SNMP, and time zone.
Clients will be directed to URL entered in the 'Home Page' field after successful login.
Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely.
Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
WAN Configuration
Configure static IP, DHCP or PPPoE client on WAN port.
LAN1 & LAN2 Configuration
Clients from LAN1 & LAN2 must login before accessing network, except those devices listed on the IP/MAC Privilege List. The LAN1 & LAN2 operates in NAT mode or Router mode.
Available options include DHCP Server and DHCP Relay.
LAN3 & LAN4 Configuration
Clients from LAN3 & LAN4 will not be authenticated. The LAN3 & LAN4 operates in NAT mode or Router mode.
Available options include DHCP Server and DHCP Relay.
Wireless Configuration
Clients from wireless must login before accessing network, except those devices listed on the IP/MAC Privilege List. The wireless operates in NAT mode or Router mode.
Available options include DHCP Server and DHCP Relay.

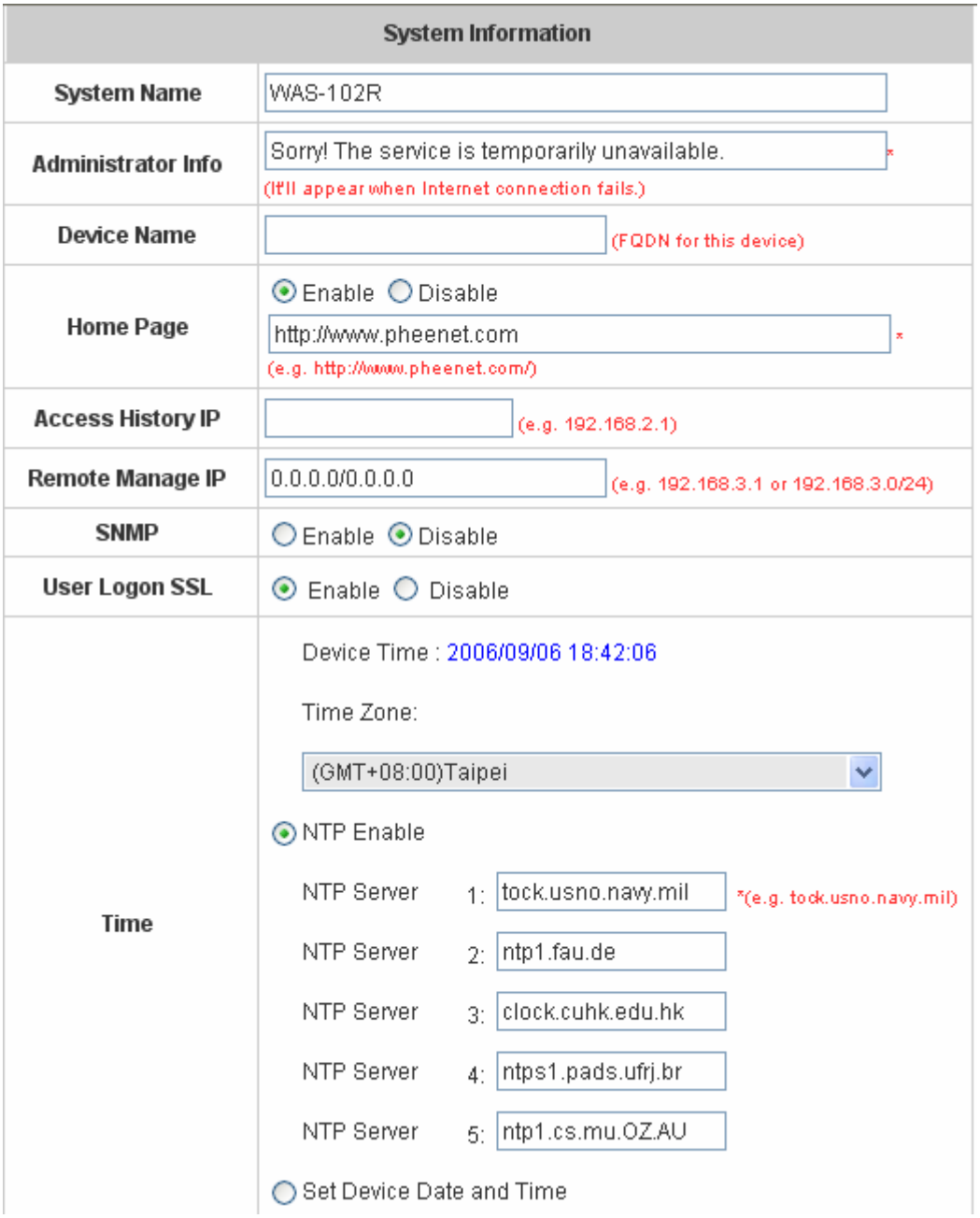
4.1.1 Configuration Wizard

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 7 steps providing a simple and easy way to go through the basic setups of WAS-102R and is served as **Quick Configuration**. Please refer to **3.2.2 Quick Configuration** for the introduction and description of **Configuration Wizard**.

Configuration Wizard
WAS-102R is an Ethernet Broadband Router with access control features ideal for hotspot, small business and enterprise networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure WAS-102R.
Run Wizard

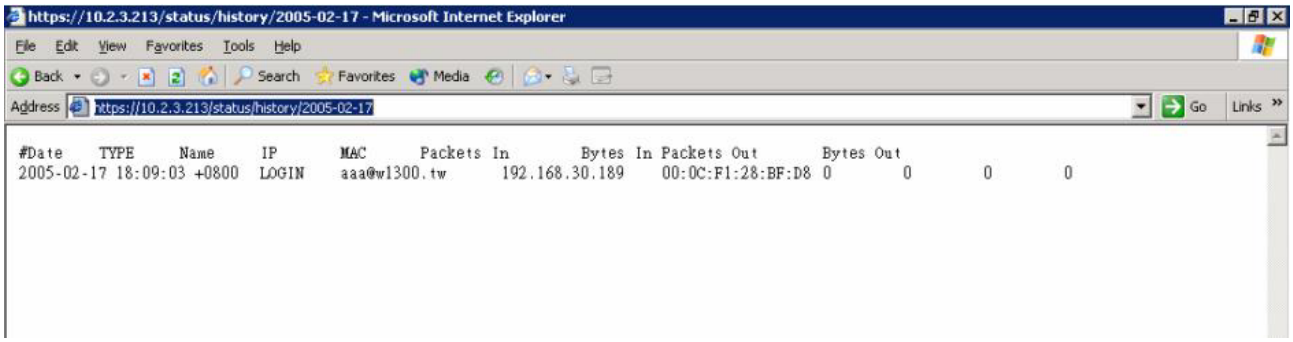
4.1.2 System Information

These are some main information about WAS-102R. Please refer to the following description for these blanks:

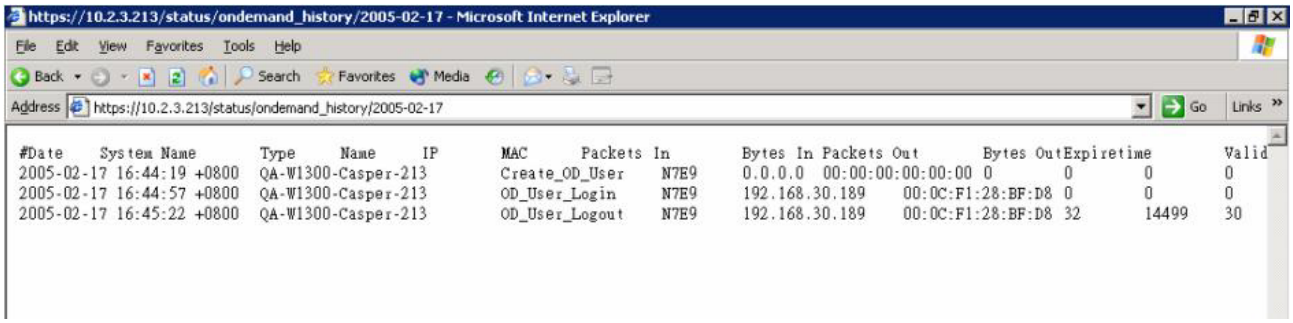


- **System Name:** Set the system's name or use the default.
- **Administrator Info:** Enter the Administrator's information here, such as administrator's name, telephone number, e-mail address, etc. If users encountered problems in the connection of the WAN port to the system, this information will appear on the user's login screen.
- **Home Page:** Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set, such as http://www.yahoo.com. Regardless of the original webpage set in the users' computers, they will be redirect to this page after login.
- **Access History IP:** Specify an IP address of the administrator's computer or a billing system to get billing history information of WAS-102R.

Traffic History：https://10.2.3.213/status/history/2005-02-17


https://10.2.3.213/status/history/2005-02-17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.2.3.213/status/history/2005-02-17
Go Links
#Date TYPE Name IP MAC Packets In Bytes In Packets Out Bytes Out
2005-02-17 18:09:03 +0800 LOGIN aaa@wl300.tw 192.168.30.189 00:0C:F1:28:BF:D8 0 0 0 0

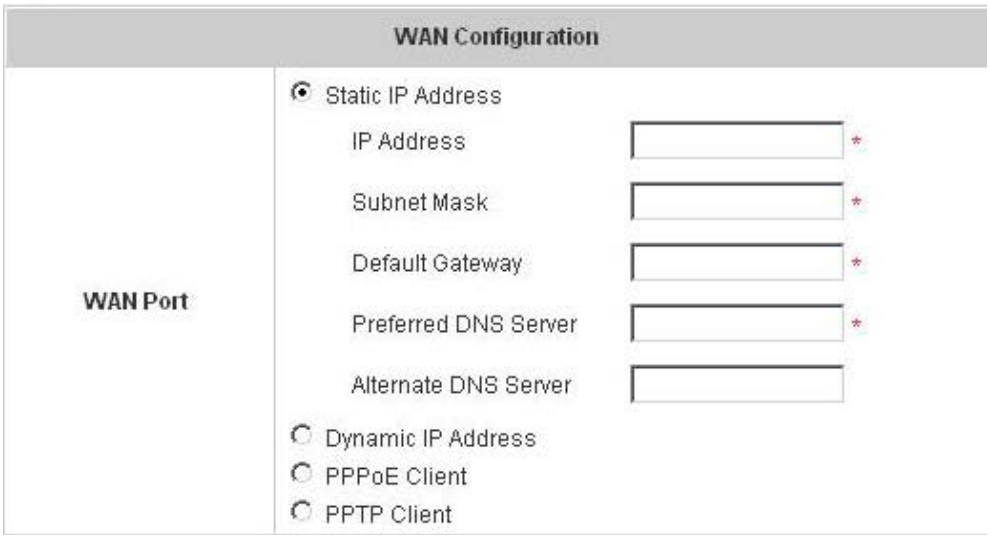
On-demand History：https://10.2.3.213/status/ondemand_history/2005-02-17


https://10.2.3.213/status/ondemand_history/2005-02-17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.2.3.213/status/ondemand_history/2005-02-17
Go Links
#Date System Name Type Name IP MAC Packets In Bytes In Packets Out Bytes Out Expiretime Valid
2005-02-17 16:44:19 +0800 QA-WL300-Casper-213 Create_OD_User N7E9 0.0.0.0 00:00:00:00:00:00 0 0 0 0
2005-02-17 16:44:57 +0800 QA-WL300-Casper-213 OD_User_Login N7E9 192.168.30.189 00:0C:F1:28:BF:D8 0 0 0
2005-02-17 16:45:22 +0800 QA-WL300-Casper-213 OD_User_Logout N7E9 192.168.30.189 00:0C:F1:28:BF:D8 32 14499 30

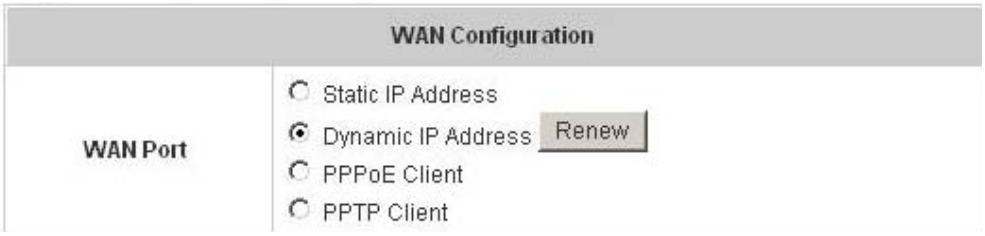
- **Remote Manage IP:** Set the IP block with a system which is able to connect to the web management interface via the authenticated port. For example, 10.2.3.0/24 means that as long as you are within the IP address range of 10.2.3.0/24, you can reach the administration page of WAS-102R.
- **SNMP:** WAS-102R supports SNMPv2. If the function is enabled, administrators can assign the Manager IP address and the SNMP community name used to access the management information base (MIB) of the system.
- **User logon SSL:** Enable to activate https (encryption) or disable to activate http (non encryption) login page.
- **Time:** WAS-102R supports NTP communication protocol to synchronize the network time. Please specify the IP address of a server in the system configuration interface for adjusting the time automatically. (Universal Time is Greenwich Mean Time, GMT). Time can be set manually by selecting **"Set Device Date and Time"**. Please enter the date and time for these fields.

4.1.3 WAN Configuration

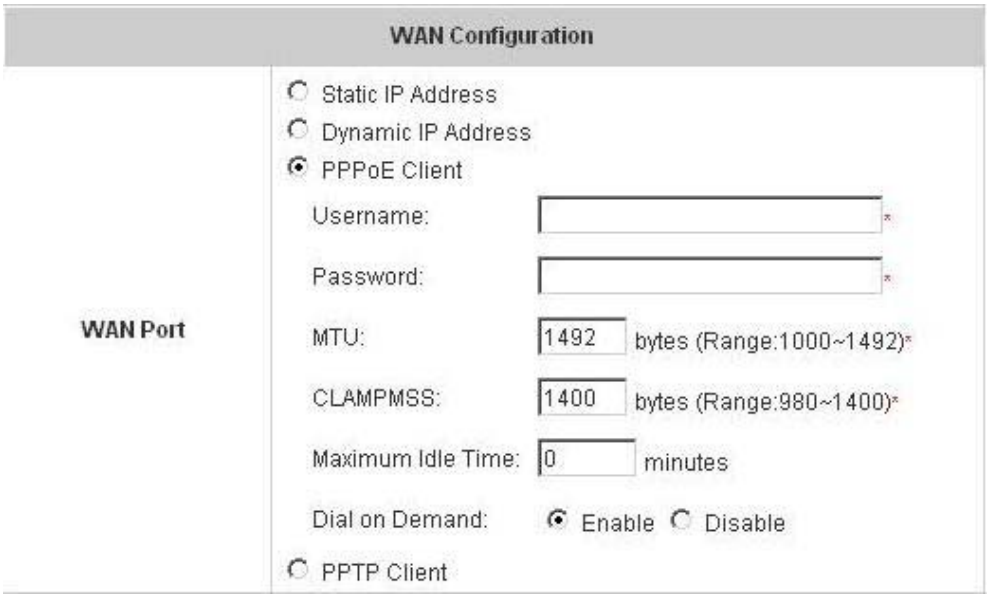
There are 4 methods of obtaining IP address for the WAN Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE** and **PPTP Client**.



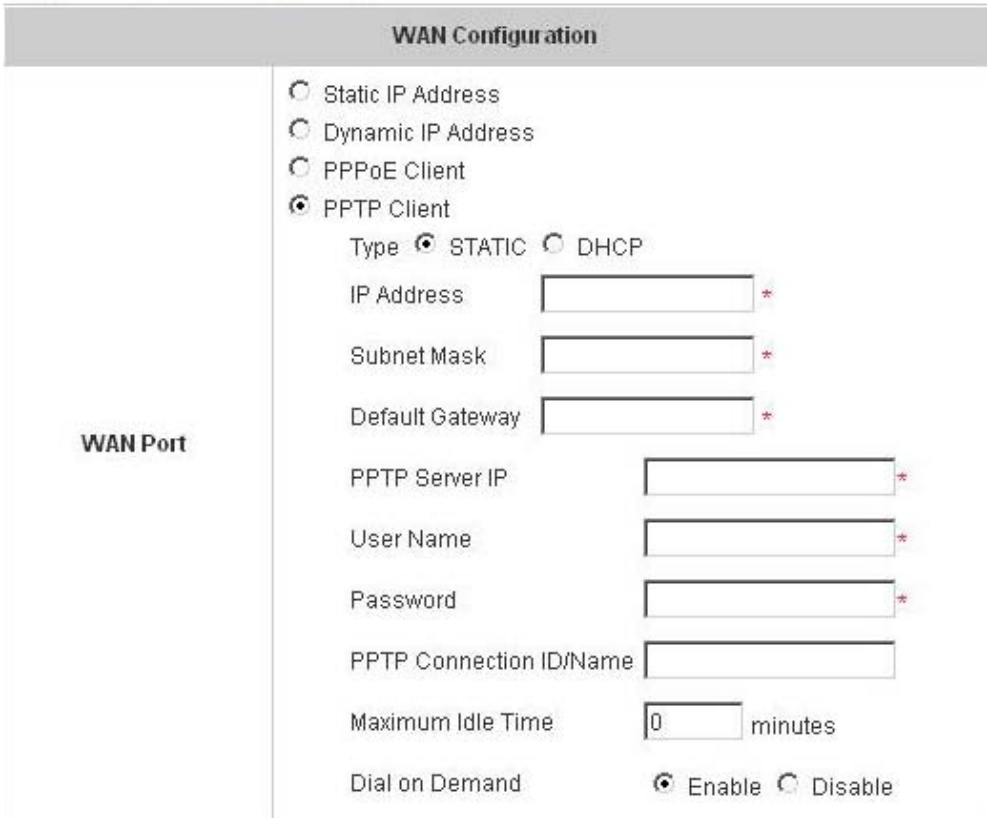
- **Static IP Address:** Manually specifying the IP address of the WAN Port is applicable for the network environment where the DHCP service is unavailable. The fields with red asterisks are required to be filled in.
  IP address: the IP address of the WAN port.
  Subnet mask: the subnet mask of the WAN port.
  Default gateway: the gateway of the WAN port.
  Preferred DNS Server: the primary DNS Server of the WAN port.
  Alternate DNS Server: The substitute DNS Server of the WAN port. This is not required.
- **Dynamic IP address:** It is only applicable for the network environment where the DHCP Server is available in the network. Click the ***Renew*** button to get an IP address.

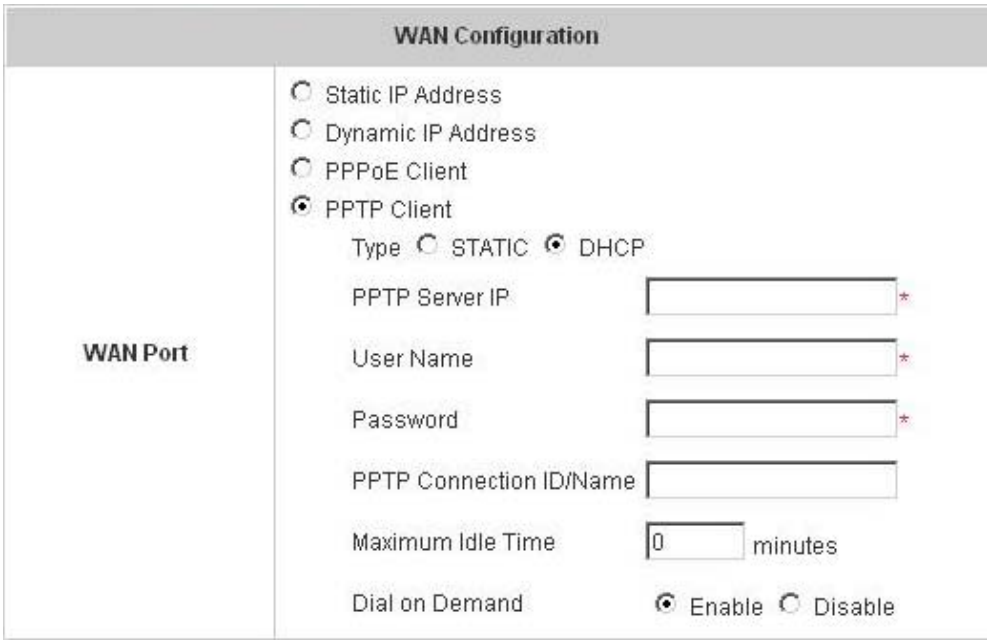


- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the **"User Name"**, **"Password"**, **"MTU"** and **"CLAMPMSS"**. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.



- **PPTP Client:** Select **STATIC** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required to be filled in. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.

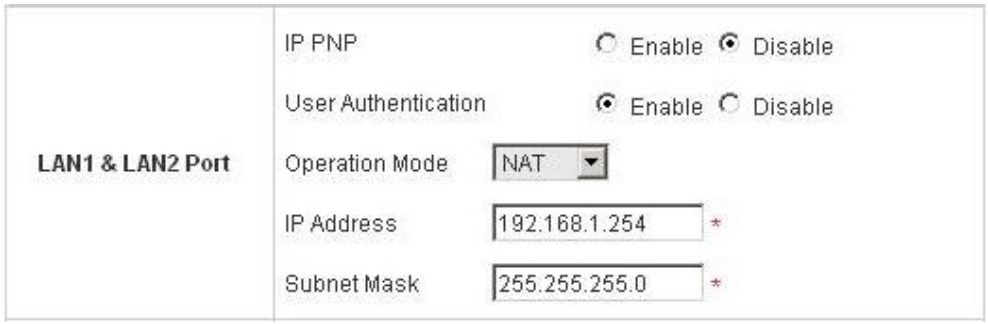




4.1.4 LAN1 & LAN2 Configuration

User authentication for the two LAN ports can be enabled or disabled.

- **LAN1 & LAN2 Port**



IP PNP: Users can use any IP address to connect to the system. Regardless of what the IP address at the user end is, users can still be authenticated through WAS-102R and access the network.

User Authentication: Choose to enable or disable this function. If **"User Authentication"** is disabled, users can access Internet without being authenticated.

Operation Mode: Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

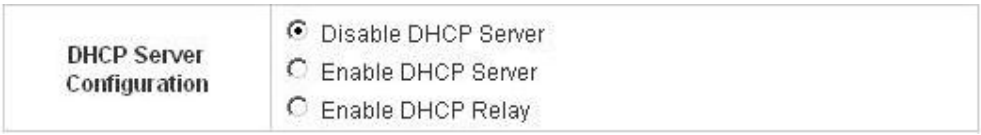
IP Address: Enter the desired IP address for the LAN1 & LAN2 port.

Subnet Mask: Enter the desired subnet mask for the LAN1 & LAN2 port.

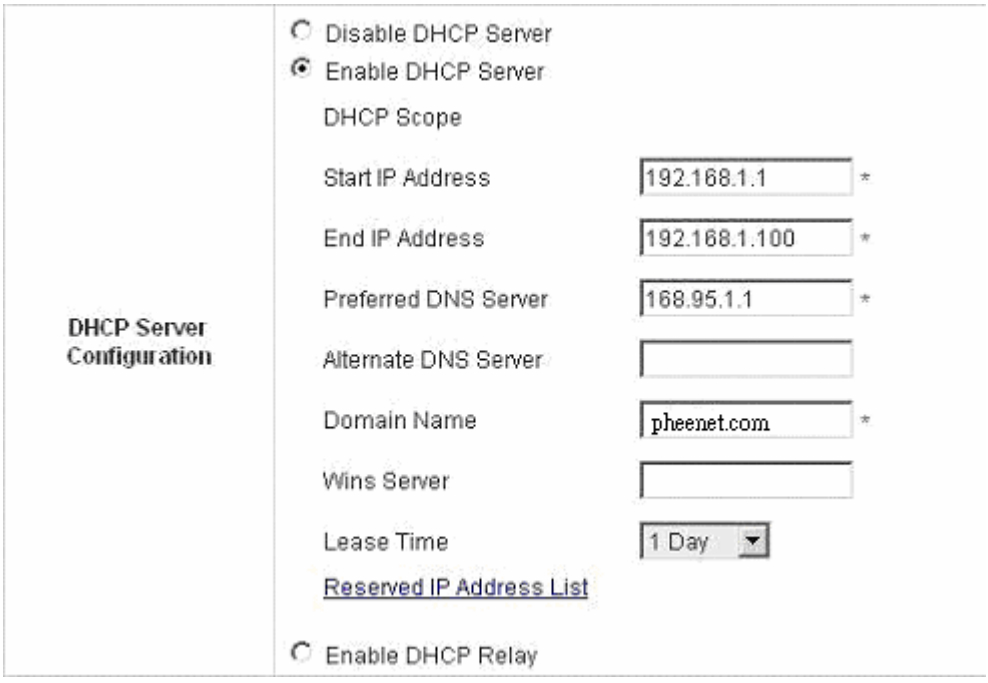
- **DHCP Server Configuration**

  There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

  1. **Disable DHCP Server:** Disable DHCP Server function.



  2. **Enable DHCP Server:** Choose **"Enable DHCP Sever"** function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.



DHCP Scope: Enter the **"Start IP Address"** and the **"End IP Address"** of this DHCP block. These fields define the IP address range that will be assigned to the Public LAN clients.

Preferred DNS Server: The primary DNS server for the DHCP.

Alternate DNS Server: The substitute DNS server for the DHCP.

Domain Name: Enter the domain name.

WINS IP Address: Enter the IP address of WINS

Lease Time: Choose the time to change the DHCP.

Reserved IP Address List: For reserved IP address settings in detail, please click the hyperlink of

Reserved IP Address. If using the **Reserved IP Address List** function for IP address outside the DHCP range is desired, click on the **Reserved IP Address List** on the management interface. Then, the setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not mandatory). Click ***Apply*** to complete the setup.

Reserved IP Address List - LAN1 & LAN2			
Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
(Total:40) First Prev Next Last			

3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. See the following figure.

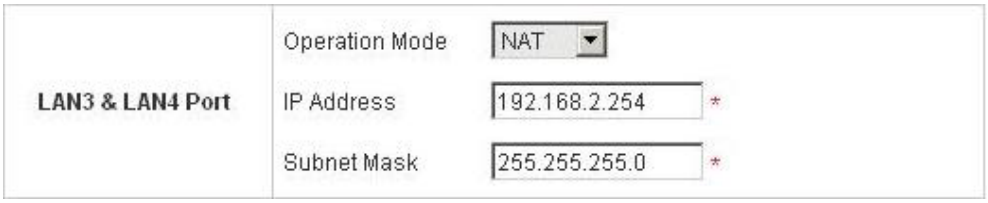
DHCP Server Configuration	○ Disable DHCP Server ○ Enable DHCP Server ◉ Enable DHCP Relay DHCP Server IP *

4.1.5 LAN3 & LAN4 Configuration

In this section, set the related configuration for LAN3/LAN4 port and DHCP server.

LAN3 & LAN4 Configuration	
LAN3 & LAN4	Operation Mode: NAT IP Address: 192.168.2.254 * Subnet Mask: 255.255.255.0 *
DHCP Server Configuration	◉ Disable DHCP Server ○ Enable DHCP Server ○ Enable DHCP Relay

- **LAN3 & LAN4 Port**



Operation Mode: Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

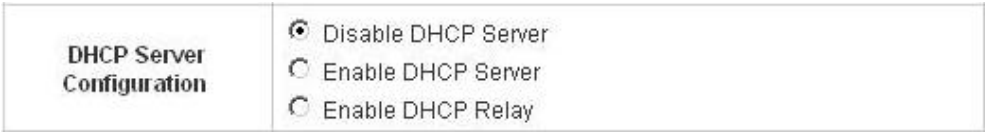
IP Address: Enter the desired IP address for the LAN3 & LAN4 port.

Subnet Mask: Enter the desired subnet mask for the LAN3 & LAN4 port.

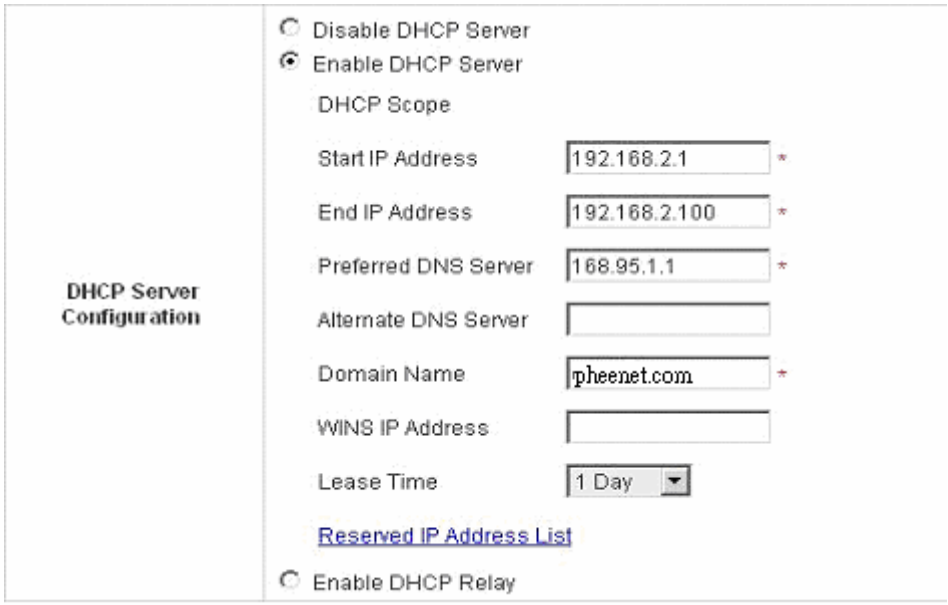
- **DHCP Server Configuration**

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable DHCP Server function.



2. **Enable DHCP Server:** Choose **"Enable DHCP Sever"** function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.



DHCP Scope: Enter the **"Start IP Address"** and the **"End IP Address"** of this DHCP block. These fields define the IP address range that will be assigned to the Private LAN clients.

Preferred DNS Server: The primary DNS server for the DHCP.

Alternate DNS Server: The substitute DNS server for the DHCP.

Domain Name: Enter the domain name.

WINS IP Address: Enter the IP address of WINS.

Lease Time: Choose the time to update the DHCP.

Reserved IP Address List: For reserved IP address settings in detail, please click the hyperlink of ***Reserved IP Address***. If using the **Reserved IP Address List** function for IP address outside the DHCP range is desired, click the **Reserved IP Address List** on the management interface. The setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not mandatory). Click ***Apply*** to complete the setup.

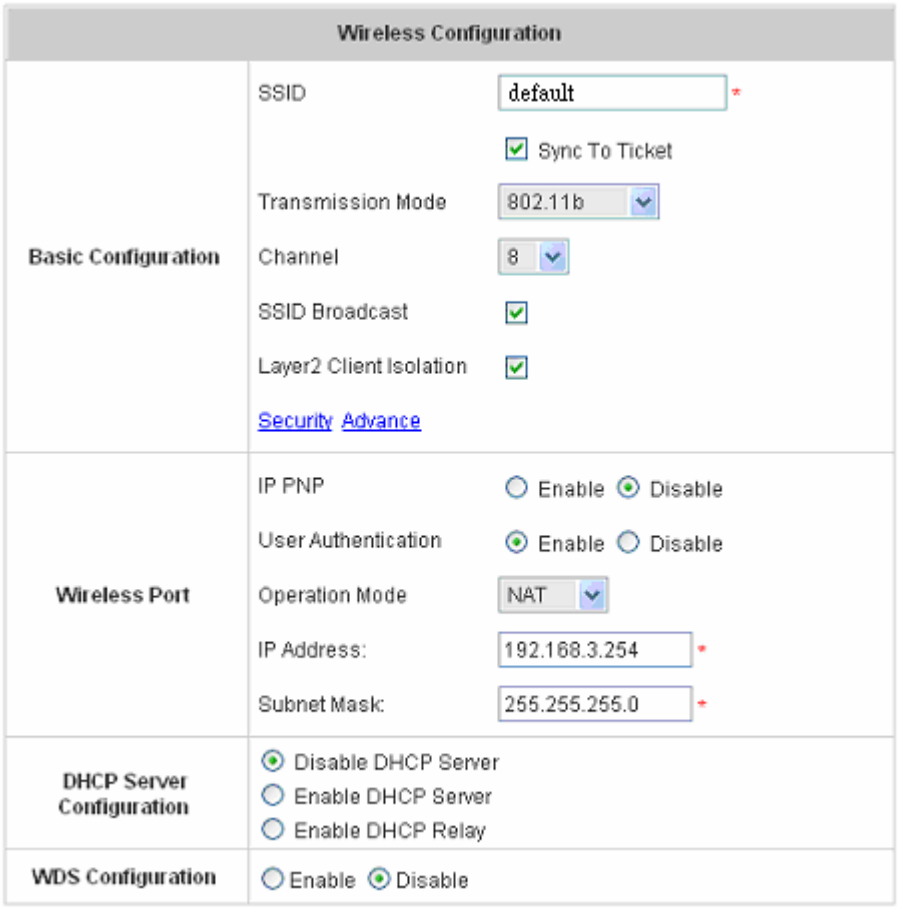
Reserved IP Address List - LAN3 & LAN4			
Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
(Total:40) First Prev Next Last			

3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. See the following figure.

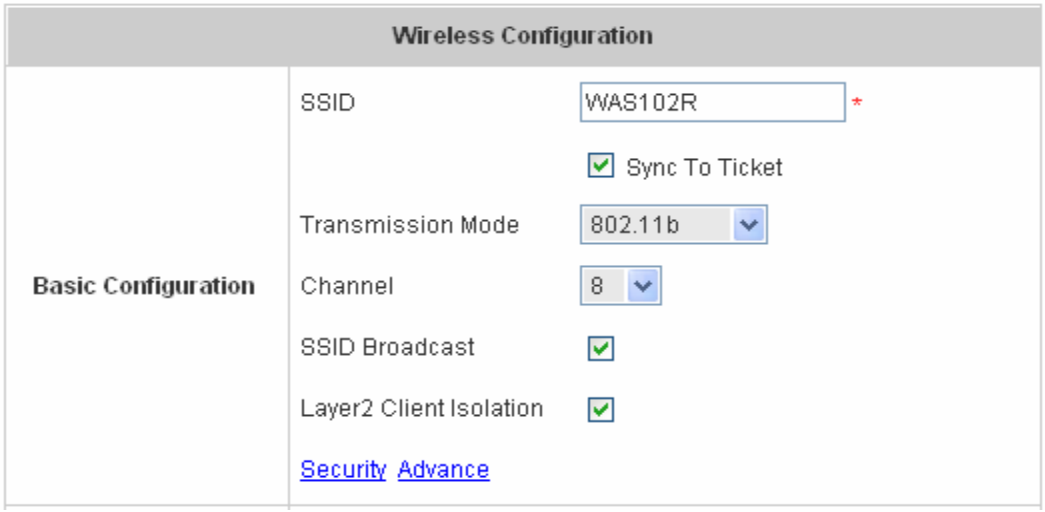
DHCP Server Configuration	○ Disable DHCP Server ○ Enable DHCP Server ◉ Enable DHCP Relay DHCP Server IP *

4.1.6 Wireless Configuration

This section is for setting related configurations for the wireless port.



- **Wireless Configuration**



SSID: The SSID is the unique name shared among all devices in a wireless network. The SSID must be the same for all devices in the wireless network. It is case sensitive, must not exceed 32 characters and may be any character on the keyboard. Administrators can give a new name in this field or use the default name.

Sync to Ticket: Synchronize the SSID of ticket with this system.

Channel: Select the appropriate channel from the list to correspond to the network settings; for example, 1 to 11 channels are suitable for the North America area. All points in the wireless network must use the same channel in order to make sure correct connection.

Transmission Mode: There are 2 modes to select from, **802.11b** (2.4G, 1~11Mbps) and **802.11 (b+g)** (2.4G, 1~11Mbps and 2.4G, 54Mbps).

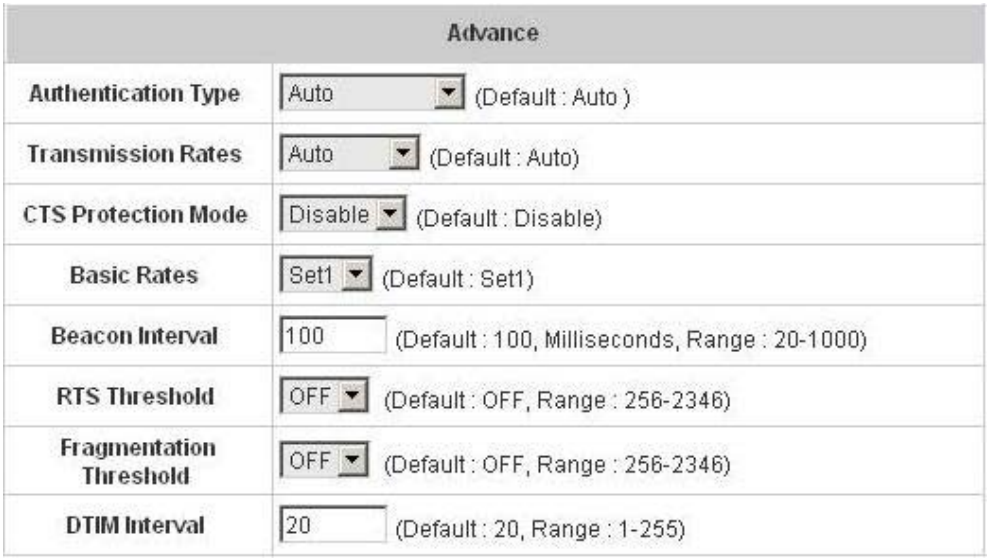
SSID Broadcast: Select to enable the SSID broadcast in the network. When configuring the network, this function may be enabled but should be disabled when configuration is finished. Since when SSID Broadcast is enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to the network.

Layer2 Client Isolation: This function can be enabled to isolate any client from each other.

Security: For security settings in detail, please click the hyperlink ***Security*** to go into the **Security** page. Choose **"Enable"** to configure the setting.

1. **WEP Key: W**ired **E**quivalent **P**rivacy. If using this function is desired, please choose **"Enable"**.
2. **WEP Key Encryption**: This is a data privacy mechanism based on a 64-bit or 128-bits shared key algorithm.
3. **Mode:** There are two types of encryption, **HEX** and **ASCII**. After selecting one of them, please enter the related information in the blanks below.

Advance: For advance settings in detail, please click the hyperlink ***Advance*** to go into the **Advance** page.



1. **Authentication Type:** The default value is **Auto**. When **"Auto"** is selected, it will auto-detect to authenticate by **Shared Key** type or **Open System** type. **Shared Key** is used such that both the sender and the recipient share a WEP key for authentication. **Open Key** is that the sender and the recipient do not share a WEP key for authentication. All points on the network must use the same authentication type.
2. **Transmission Rates:** The default value is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of this particular wireless network. Select from a range of transmission speeds or keep the default setting, **Auto**, to make the Access Point use the fastest possible data rate automatically.
3. **CTS Protection Mode:** The default value is **Disable**. When enabled, a protection mechanism will ensure that the 802.11b devices can connect to Access Point and not be affected by many other 802.11g devices existing at the same time. However, the performance of this 802.11g devices may decrease.
4. **Basic Rate:** The basic rate offers three options, **All**, **Set1** and **Set2** and the default value is **Set1**. Depending on the wireless mode selected, WAS-102R will deliver a pre-defined data rate. Select **"All"** to activate all transmission rates to be compatible with the majority of the devices.
5. **Beacon Interval:** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the signal transmission occurs between the access point and the wireless network.
6. **RTS Threshold: R**eady **T**o **S**end threshold. The range is from 256 to 2346 and the default is **OFF**. The administrator could set the value which is the time to wait before sending another packet. It is recommended that the value remains in the range of 256 to 2346.
7. **Fragmentation Threshold:** The range is from 256 to 2346 and the default is **OFF**. The value specifies the maximum size of packet allowed before data is fragmented into multiple packets. It should be remained in the range of 256 to 2346. A smaller value results smaller packets but with a larger numbers of packets in transmission.

8. **DTIM Interval:** This function indicates the interval of the **D**elivery **T**raffic **I**ndication **M**essage (DTIM). DTIM is a countdown function to inform clients to listen to broadcast and multicast messages. When an Access Point has buffered broadcast or multicast message from an associated client, it sends the next DTIM at this interval rate (from 1~255), the client will hear the beacons.

- **Wireless Configuration**

IP PNP: Use any IP address to connect to the system. Regardless of what the IP address at the users end is, they can still be authenticated through WAS-102R and access the network.

User Authentication: If **"User Authentication"** is disabled, **"Specific Route Profile"** needs to be specified for the users to access Internet.

Operation Mode: Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

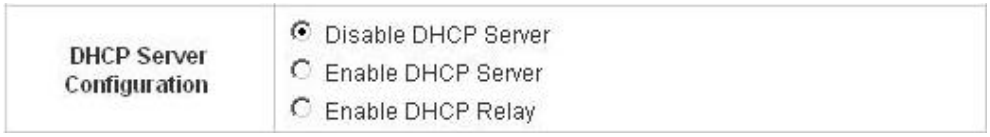
IP Address: Enter desired IP address for the wireless port.

Subnet Mask: Enter desired subnet mask for the wireless port.

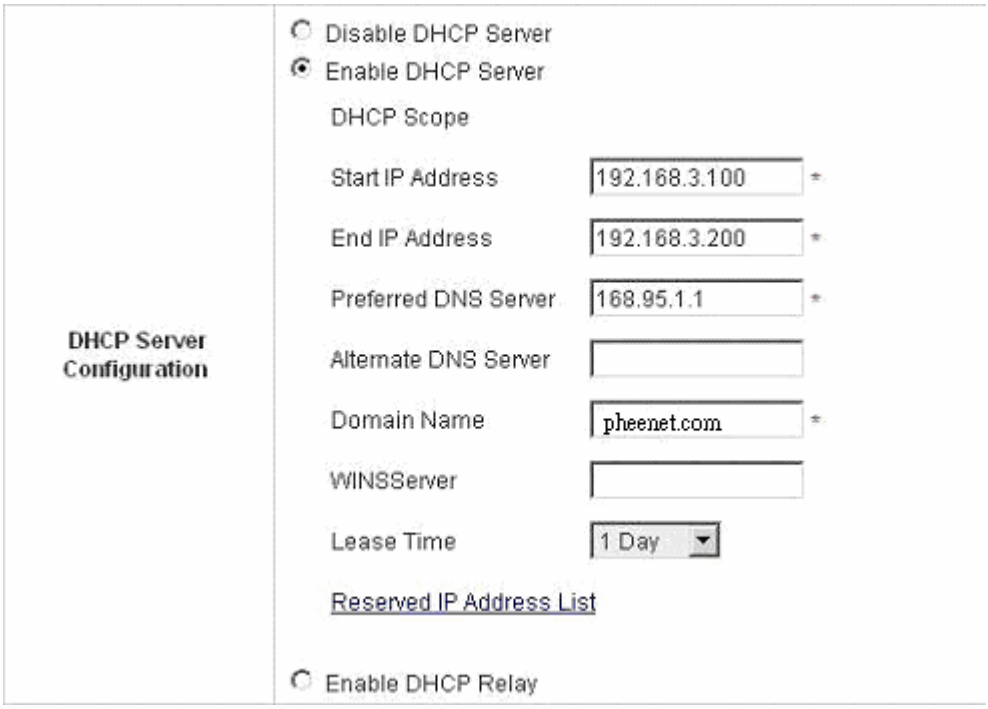
- **DHCP Server Configuration**

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable the DHCP Server function.



2. **Enable DHCP Server:** Choose **"Enable DHCP Sever"** function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.



DHCP Scope: Enter the **"Start IP Address"** and the **"End IP Address"** of this DHCP block. These fields define the IP address range that will be assigned to the Wireless LAN clients.

Preferred DNS Server: The primary DNS server for the DHCP.

Alternate DNS Server: The substitute DNS server for the DHCP.

Domain Name: Enter the domain name.

WINS IP Address: Enter the IP address of WINS.

Lease Time: Choose the time to change the DHCP.

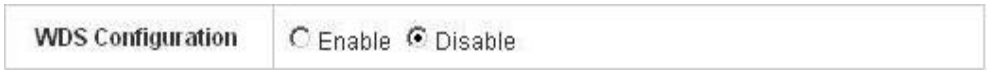
Reserved IP Address List: For reserved IP address settings in detail, please click the hyperlink of ***Reserved IP Address***. If using the **Reserved IP Address List** function for IP address outside the DHCP range is desired, click on the **Reserved IP Address List** on the management interface. The setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not mandatory). Click ***Apply*** to complete the setup.

Reserved IP Address List -- Wireless			
Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			

3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. See the following figure.

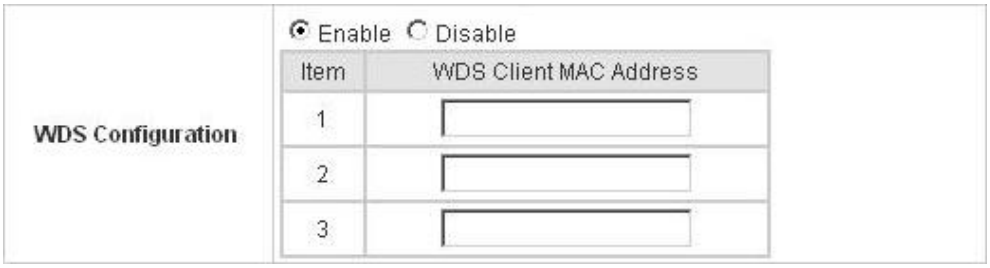
- **WDS configuration**

This function can extend the range of accessing the network. It has to work with a repeater. A repeater is a peripheral device supporting WAS-102R to extend the wireless access by receiving requests from APs or clients and passing the requests to WAS-102R to obtain authentication.



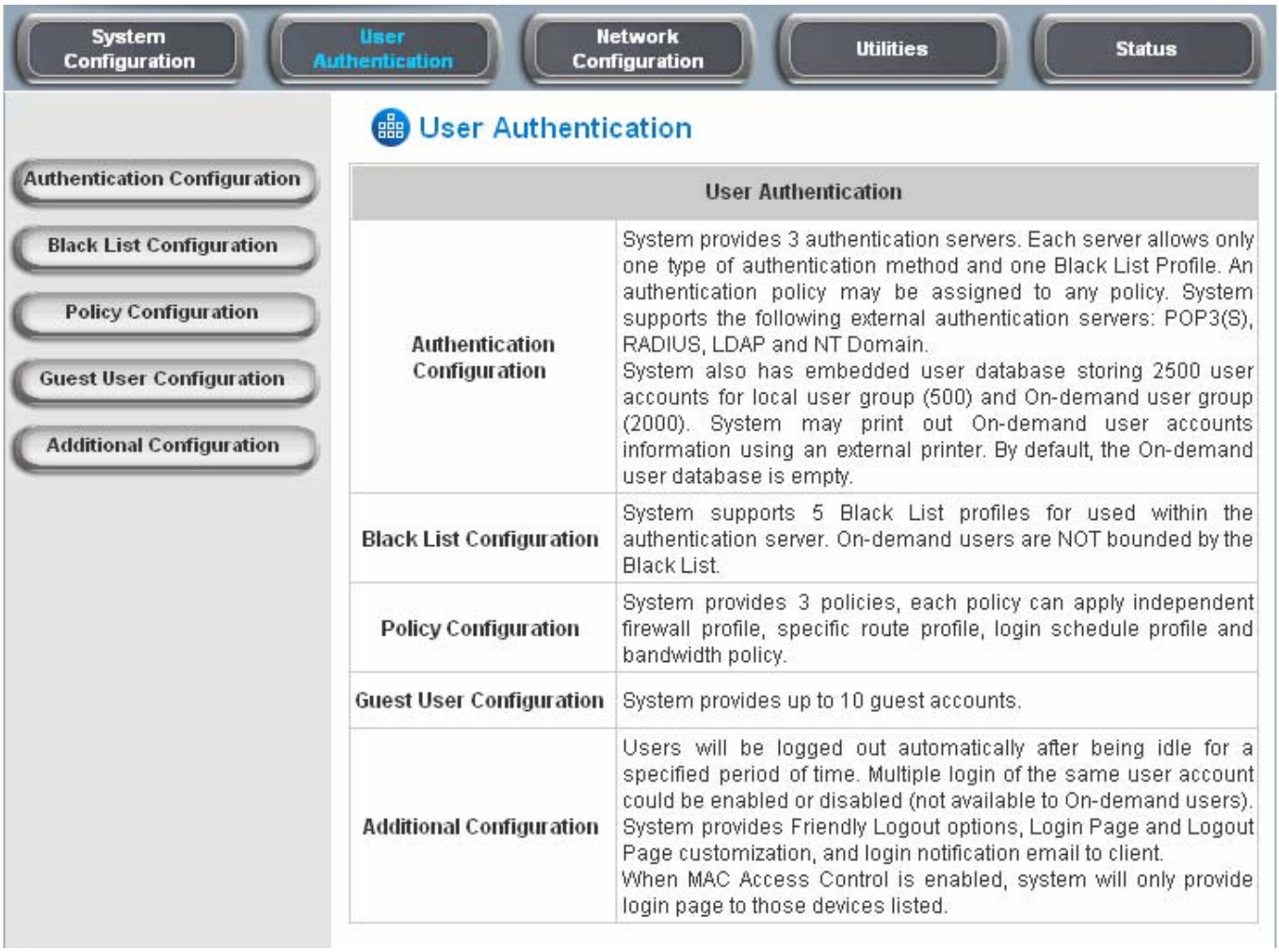
When "Enable" is clicked, there will be a warning box showing up.

If this function is enabled, please enter the MAC address of repeater in the blanks. A maximum of three repeaters are supported.



4.2 User Authentication

This section includes the following functions: **Authentication Configuration**, **Black List Configuration**, **Policy Configuration**, **Guest User Configuration** and **Additional Configuration**.


System Configuration
User Authentication
Network Configuration
Utilities
Status
Authentication Configuration
Black List Configuration
Policy Configuration
Guest User Configuration
Additional Configuration
User Authentication
User Authentication
Authentication Configuration
System provides 3 authentication servers. Each server allows only one type of authentication method and one Black List Profile. An authentication policy may be assigned to any policy. System supports the following external authentication servers: POP3(S), RADIUS, LDAP and NT Domain.
System also has embedded user database storing 2500 user accounts for local user group (500) and On-demand user group (2000). System may print out On-demand user accounts information using an external printer. By default, the On-demand user database is empty.
Black List Configuration
System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.
Policy Configuration
System provides 3 policies, each policy can apply independent firewall profile, specific route profile, login schedule profile and bandwidth policy.
Guest User Configuration
System provides up to 10 guest accounts.
Additional Configuration
Users will be logged out automatically after being idle for a specified period of time. Multiple login of the same user account could be enabled or disabled (not available to On-demand users).
System provides Friendly Logout options, Login Page and Logout Page customization, and login notification email to client.
When MAC Access Control is enabled, system will only provide login page to those devices listed.

4.2.1 Authentication Configuration

This function is to configure the settings for 802.1x authentication, authentication server, and on-demand user authentication.

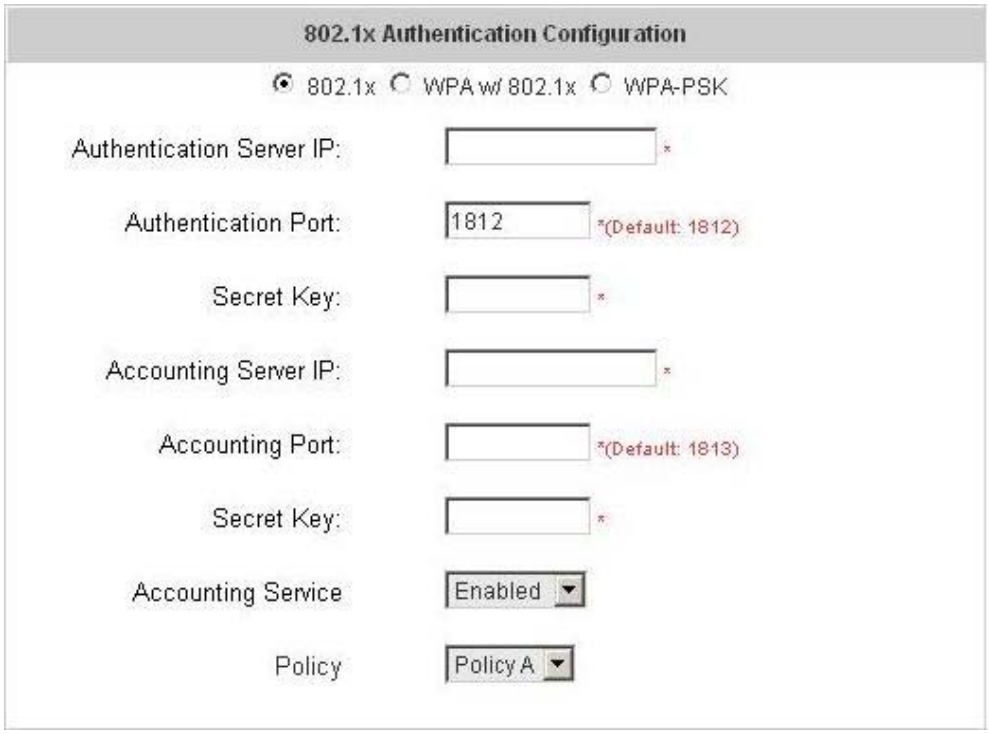
802.1x Authentication Configuration					
802.1x Authentication Configuration					☐
Authentication Server Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
Server 1	LOCAL	Postfix1	Policy A	○	☐
Server 2	POP3	Postfix2	Policy A	○	☐
Server 3	LDAP	Postfix3	Policy A	○	☐
On-demand User	ONDEMAND	bonalinx	Policy A	◉	☑

- **802.1x Authentication Configuration**

802.1x Authentication Configuration	
802.1x Authentication Configuration	☑

There are two kinds of 802.1x authentication methods and one encryption mechanism: **802.1x**, **WPA w/ 802.1x** and **WPA-PSK**. Click the hyperlink ***802.1x Authentication Configuration*** to set the related configurations. After completing and clicking ***Apply*** to save the settings, go back to the previous page to check the item box next to ***802.1x Authentication Configuration*** to enable this function. When using 802.1x authentications, the RADIUS attributes such as idle timeout or session timeout have no effect.

1. **802.1x:** Enable the 802.1x authentication method. The fields with red asterisks are required to be filled in.



Authentication Server IP: The IP address or domain name of the Authentication server.

Authentication Port: The port of the authentication server. The default value is 1812.

Secret Key: The secret key of the authentication sever for encryption and decryption.

Accounting Server IP: The IP address or domain name of the accounting server.

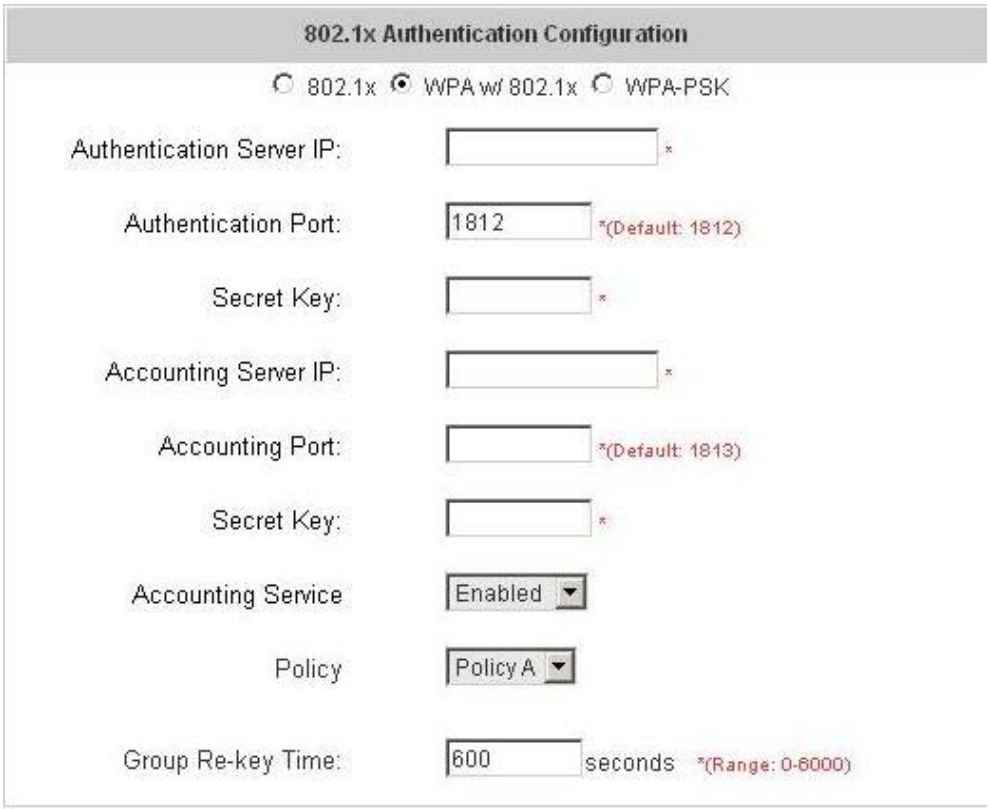
Account Port: The port of the accounting server. The default value is 1813.

Secret Key: The secret key of the accounting sever for encryption and decryption.

Accounting Service: Enable or disable accounting service.

Policy: There are three policies to select from.

2. **WPA x/802.1x:** Enable the supported WPA-Enterprise, Wireless Protection Access with 802.1x.



Authentication Server IP: The IP address or domain name of the Authentication server.

Authentication Port: The port of the authentication server. The default value is 1812.

Secret Key: The secret key of the authentication sever for encryption and decryption.

Accounting Server IP: The IP address or domain name of the accounting server.

Account Port: The port of the accounting server. The default value is 1813.

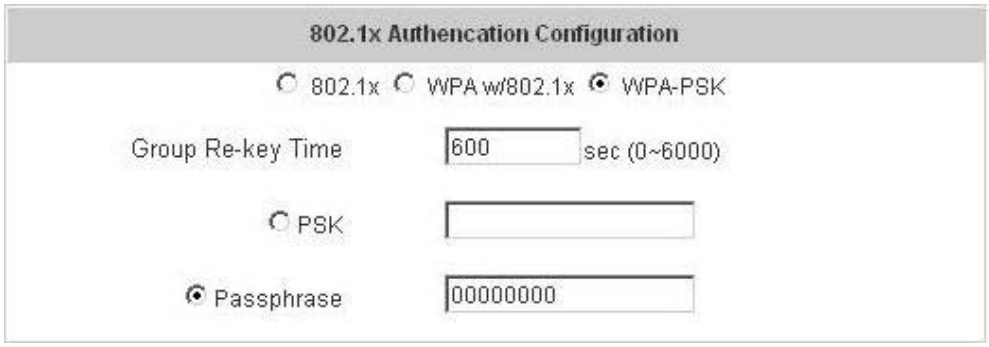
Secret Key: The secret key of the accounting sever for encryption and decryption.

Accounting Service: Enable or disable accounting service.

Policy: There are three policies to select from.

Group Re-key Time: Time interval for re-keying broadcast/multicast keys in seconds. The maximum is 6000 sec.

3. **WPA-PSK: W**ireless **P**rotection **A**ccess-**P**re**S**hared **K**ey, a kind of encryption mechanism supporting WPA-SOHO. When using WPA-PSK, there is no user authentication required.



Group Re-key Time: Time interval for re-keying broadcast/multicast keys in seconds. The maximum is 6000 sec.

PSK: The **P**re-**S**hared **K**ey uses 64 hexadecimal.

Passphrase: A kind of password using 8 to 63 ASCII characters.

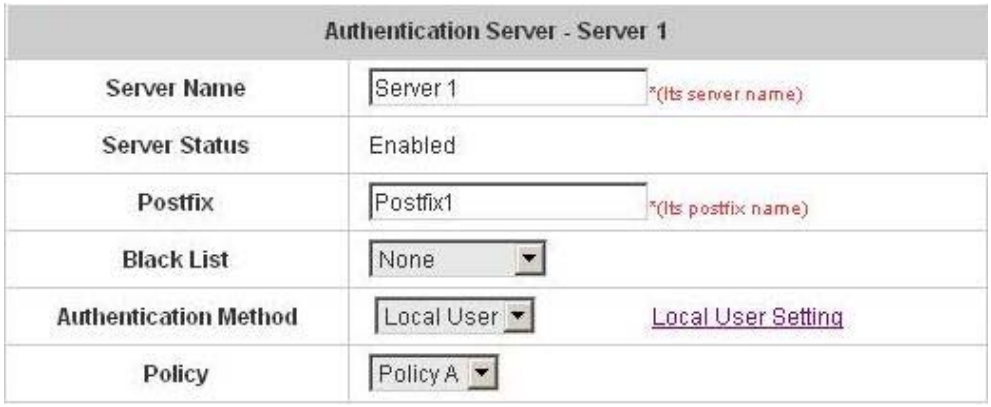
Attention: *After clicking* ***Apply****, there will be a restart message. You must click* ***Restart*** *to apply the settings.*

- **Authentication Server Configuration**

  The system provides 3 servers and one on-demand server that the administrator can apply with different policy. Click on the server name to set the related configurations for that particular server. After completing and clicking ***Apply*** to save the settings, go back to the previous page to choose a server to be the default server and enable or disable any server on the list. Users can log into the default server without the postfix to allow faster login process.

802.1x Authentication Configuration					
802.1x Authentication Configuration					☐
Authentication Server Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
Server 1	LOCAL	Postfix1	Policy A	○	☐
Server 2	LOCAL	Postfix2	Policy A	○	☐
Server 3	LOCAL	Postfix3	Policy A	○	☐
On-demand User	ONDEMAND	pheenet	Policy A	◉	☑

1. **Server 1~3:** There are 5 kinds of authentication methods, Local User, POP3, RADIUS, LDAP and NTDomain to setup from.



Server Name: Set a name for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

Sever Status: The status shows that the server is enabled or disabled.

Postfix: Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

Warning: *The Policy Name cannot contain these words: MAC and IP.*

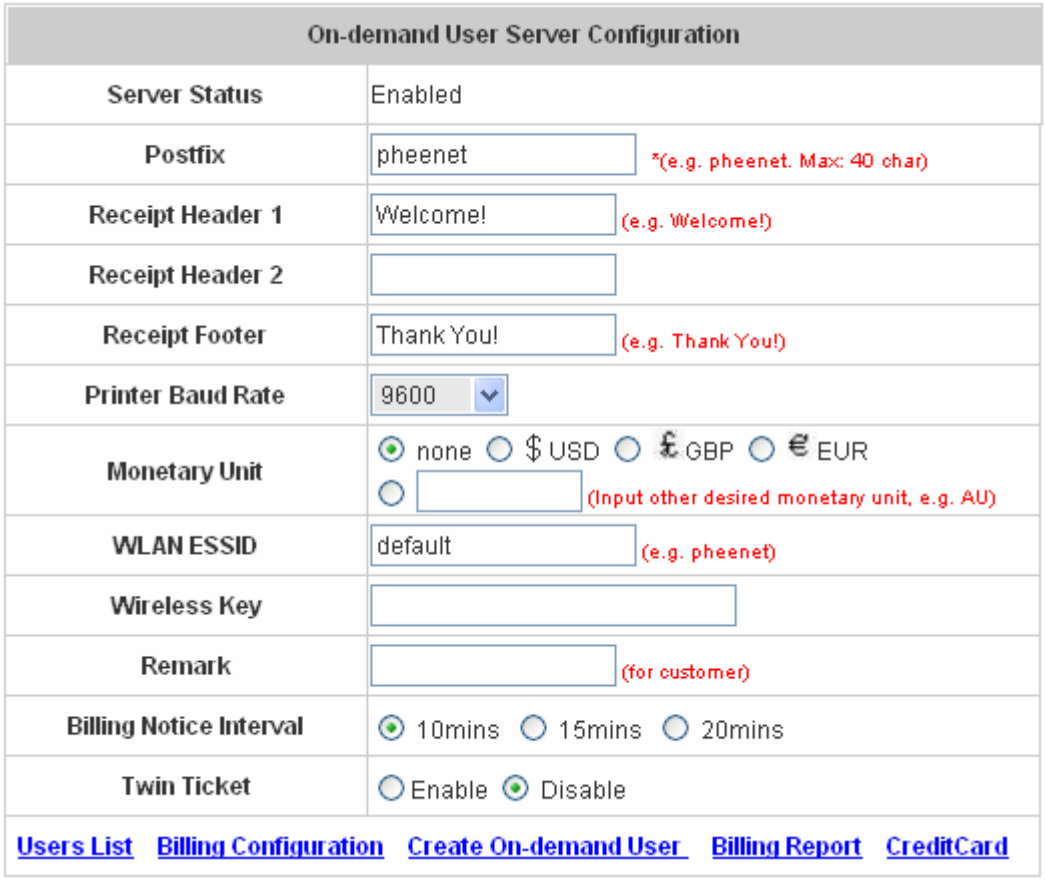
Black List: There are 5 sets of the black lists. Select one of them or choose **"None"**. Please refer to **4.2.2 Black List Configuration**

Authentication Methods: There are 5 authentication methods, **Local**, **POP3**, **RADIUS**, **LDAP** and **NT Domain** to configure from. Select the desired method and click the link besides the pull-down menu for more advanced configuration. For more details, please refer to **4.2.1.1~5 Authentication Method**.

Notice: *Enabling two or more servers of the same authentication method is not allowed.*

Policy: There are 3 policies to choose from to apply to this particular server.

2. **On-demand User:** This is for the customer's need in a store environment. When the customers need to use wireless Internet in the store, they have to get a printed receipt with username and password from the store to log in the system for wireless access. There are 2000 On-demand User accounts available.



Server Status: The status shows that the server is enabled or disabled.

Postfix: Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

Receipt Header: There are two fields, **Receipt Header 1** and **Receipt Header 2**, for the receipt's header. Enter receipt header message or use the default.

Receipt Footer: Enter receipt footer message here or use the default.

Printer Baud Rate: Select the desired transmission baud rate. The default value is 9600.

Monetary Unit: Select the desired monetary unit.

Policy Name: Select a policy for the on-demand user.

WLAN ESSID: Enter the ESSID of the AP. Administrators can supply a new name or use the default name.

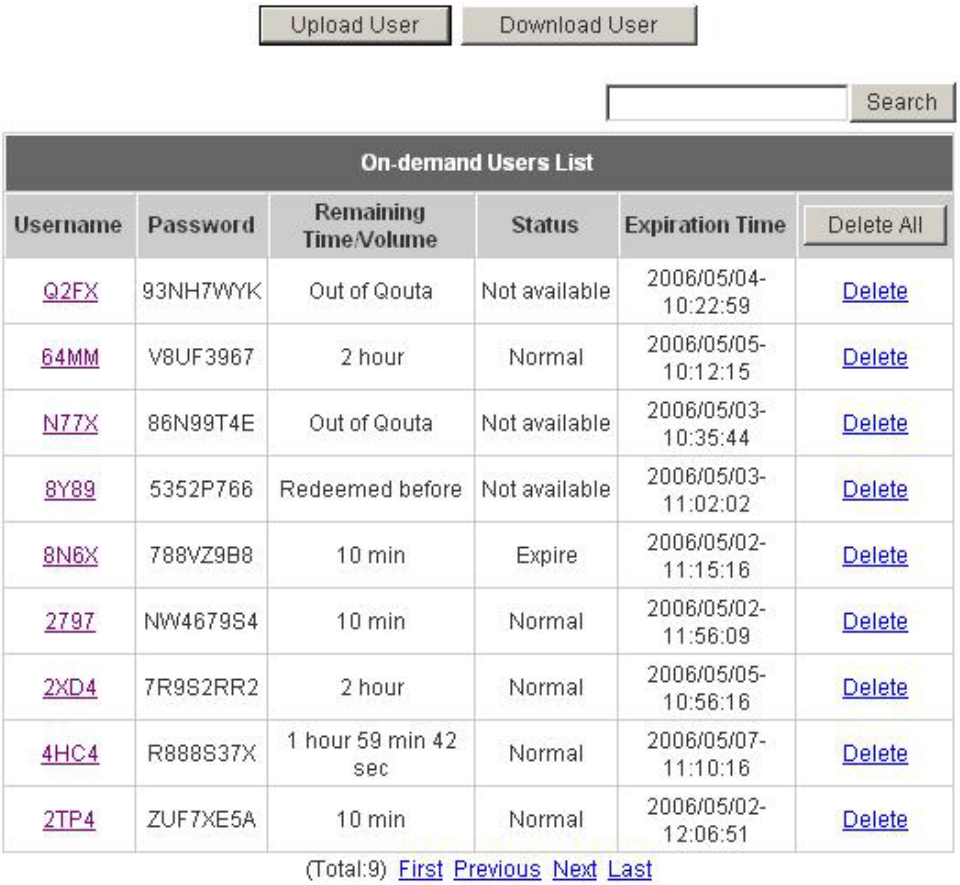
WEP Key: Enter the WEP key of the AP.

Remark: Enter any additional information that will appear at the bottom of the receipt.

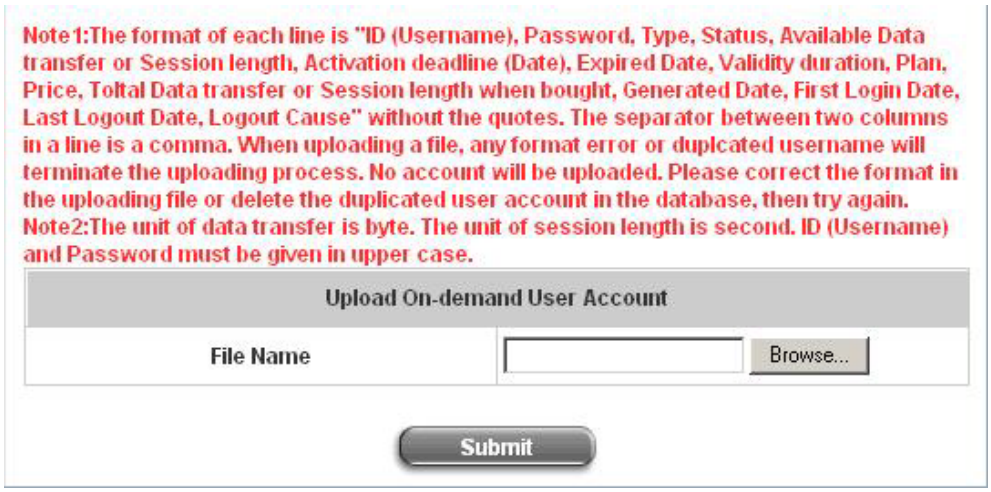
Billing Notice Interval: While the on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval defined here.

Twin Ticket: Enable this function to print duplicate receipts.

User List: Click to enter the **On-demand User List** page. In the **On-demand User List**, detailed information will be documented here. By default, the On-demand user database is empty.


Upload User
Download User
Search
On-demand Users List
Username
Password
Remaining Time/Volume
Status
Expiration Time
Delete All
Q2FX 93NH7WYK Out of Qouta Not available 2006/05/04-10:22:59 Delete
64MM V8UF3967 2 hour Normal 2006/05/05-10:12:15 Delete
N77X 86N99T4E Out of Qouta Not available 2006/05/03-10:35:44 Delete
8Y89 5352P766 Redeemed before Not available 2006/05/03-11:02:02 Delete
8N6X 788VZ9B8 10 min Expire 2006/05/02-11:15:16 Delete
2797 NW4679S4 10 min Normal 2006/05/02-11:56:09 Delete
2XD4 7R9S2RR2 2 hour Normal 2006/05/05-10:56:16 Delete
4HC4 R888S37X 1 hour 59 min 42 sec Normal 2006/05/07-11:10:16 Delete
2TP4 ZUF7XE5A 10 min Normal 2006/05/02-12:06:51 Delete
(Total:9) First Previous Next Last

- **Upload User:** Click this to enter the **Upload User** interface. Click the ***Browse*** button to select the text file for the user account upload. Then click ***Submit*** to complete the upload process.

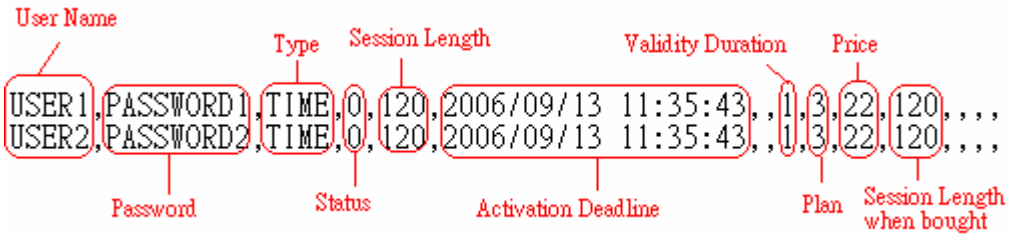

Note1:The format of each line is "ID (Username), Password, Type, Status, Available Data transfer or Session length, Activation deadline (Date), Expired Date, Validity duration, Plan, Price, Toltal Data transfer or Session length when bought, Generated Date, First Login Date, Last Logout Date, Logout Cause" without the quotes. The separator between two columns in a line is a comma. When uploading a file, any format error or duplcated username will terminate the uploading process. No account will be uploaded. Please correct the format in the uploading file or delete the duplicated user account in the database, then try again.
Note2:The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.
Upload On-demand User Account
File Name
Browse...
Submit

The uploading file should be a text file and the format of each line is ***" ID (Username), Password, Type, Status, Available Data transfer or Session length, Activation deadline (Date), Expired Date, Validity duration, Plan, Price, Total Data transfer or Session length when bought, Generated Date, First Login Date, Last Logout Date, Logout Cause"*** without the quotes. The separator between two columns in a line is a comma. When uploading a file, any format error or duplicated username will terminate the uploading process and no account will be uploaded. Please correct the

format in the uploading file or delete the duplicated user account in the database, then try again. The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.

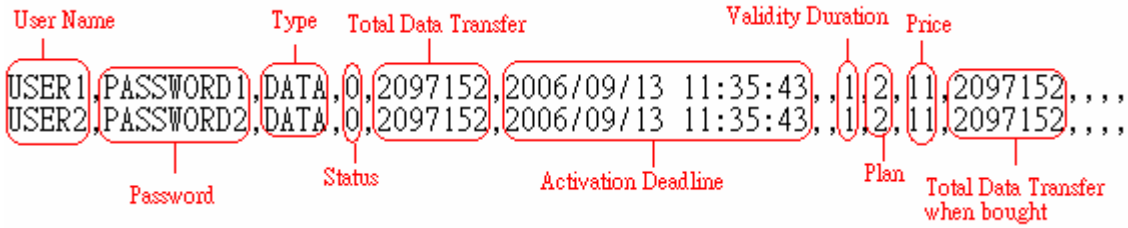
Example1: For Session Length type

The ***Type*** must be written as **TIME**, Set Status must be set as **0**. Set ***Session Length*** in seconds. ***Activation Deadline*** must be in the format of yyyy/mm/dd hh:mm:ss. Set ***Validity Duration*** as **1**, and give a ***Plan*** that's already been generated and enabled from **Billing Configuration** page. Provide a price in any monetary unit defined in **On-demand User Server Configuration** page. Finally, set ***Session Length when bought*** the same as ***Session Length***. Leave other fields blank.

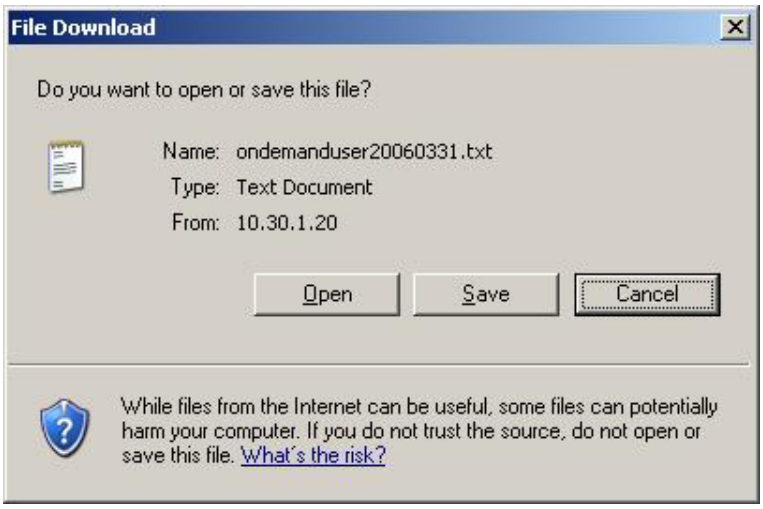


Example2: For Total Data Transfer type

The ***Type*** must be written as **DATA**, Set Status must be set as **0**. Set ***Total Data Transfer*** in bytes. ***Activation Deadline*** must be in the format of yyyy/mm/dd hh:mm:ss. Set ***Validity Duration*** as **1**, and give a ***Plan*** that's already been generated and enabled from **Billing Configuration** page. Provide a price in any monetary unit defined in **On-demand User Server Configuration** page. Finally, set ***Total Data Transfer when bought*** the same as ***Session Length***. Leave other fields blank.



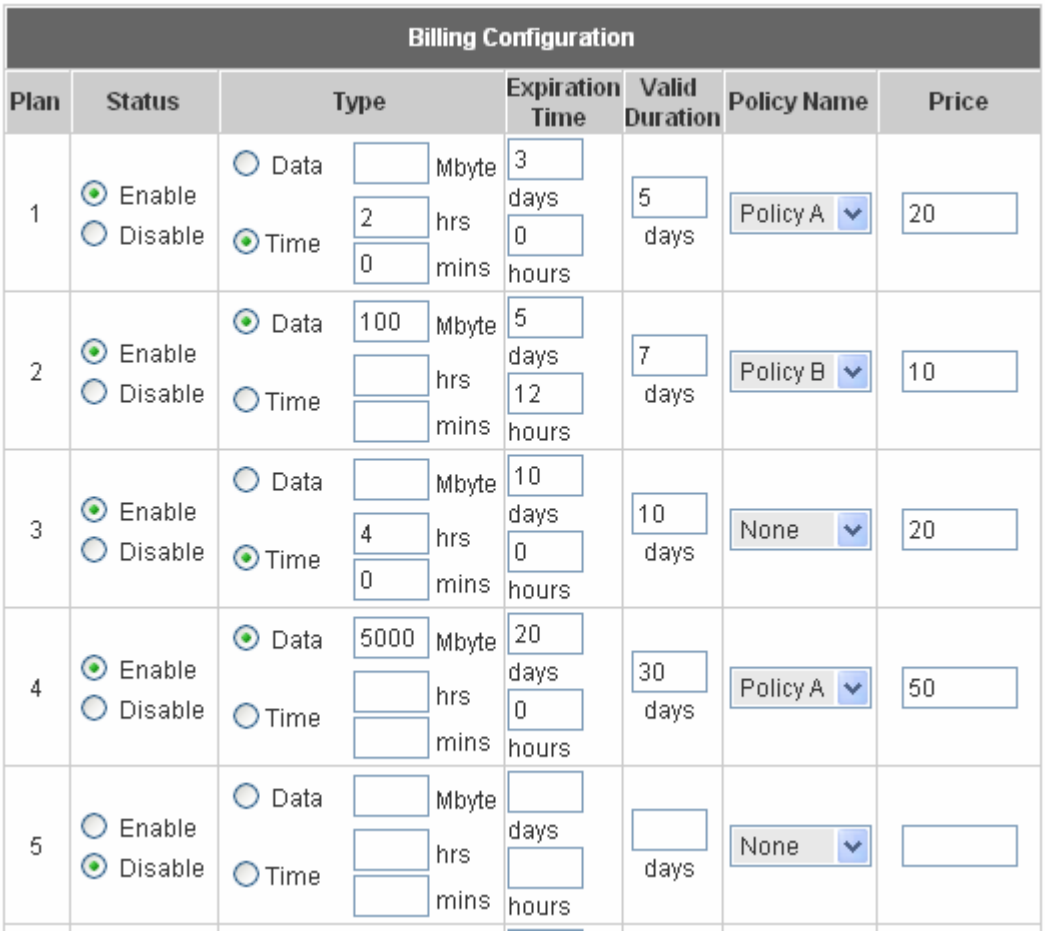
- **Download User:** Click this to create a .txt file and then save it on disk.


File Download
Do you want to open or save this file?
Name: ondemanduser20060331.txt
Type: Text Document
From: 10.30.1.20
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

- **Search:** Enter a keyword of a username that needs to be searched in the text field and click this button to perform the search. All usernames matching the keyword will be listed.

- **Username:** The login name of the on-demand user.
- **Password:** The login password of the on-demand user.
- **Remain Time/Volume:** The total time/Volume that the user can use currently.
- **Status:** The status of the account. Normal indicates that the account is not in-use and not overdue. Online indicates that the account is in-use and not overdue. Expire indicates that the account is overdue and cannot be used.
- **Expire Time:** The expiration time of the account.
- **Del All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

Billing Configuration: Billing Configuration: Click this to enter the **Billing Configuration** page. In the **Billing Configuration** screen, Administrator may configure up to 10 billing rules.

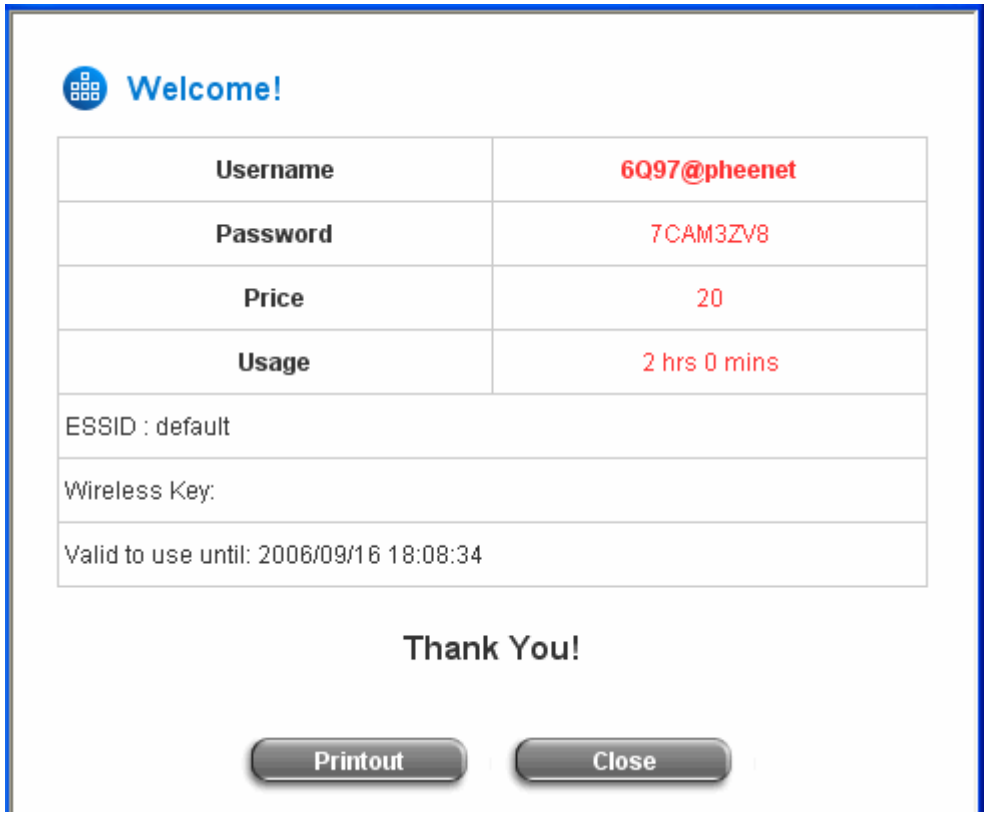


- **Status:** Select to enable or disable this billing rule.
- **Type:** Set the billing rule by **"Data"** (the maximum volume allowed is 9,999,999 Mbyte) or **"Time"** (the maximum days allowed is 999 days).
- **Expired Info:** This is the duration of time that the user can use the account after the activation of the account. After this duration, the account will self-expires.
- **Valid Duration:** This is the duration of time that the user needs to activate the account after the generation of the account. If the account is not activated during this duration, the account will self-expires.
- **Price:** The price charged for this billing rule.

Create On-demand User: Click this to enter the **On-demand User Generate** page.

Create On-demand User				
Plan	Type	Price	Status	Function
1	2 hrs 0 mins	20	Enabled	Create
2	N/A	N/A	Disabled	Create
3	N/A	N/A	Disabled	Create
4	N/A	N/A	Disabled	Create
5	N/A	N/A	Disabled	Create
6	N/A	N/A	Disabled	Create
7	N/A	N/A	Disabled	Create
8	N/A	N/A	Disabled	Create
9	N/A	N/A	Disabled	Create
0	N/A	N/A	Disabled	Create

Pressing the ***Create*** button for the desired rule, an On-demand user will be created, then click ***Printout*** to print a receipt which will contain this on-demand user's information.



Billing Report: Click this to enter the **On-demand Summary report** page. In **On-demand users Summary report** page, Administrator can get a complete report or a report of a particular period.

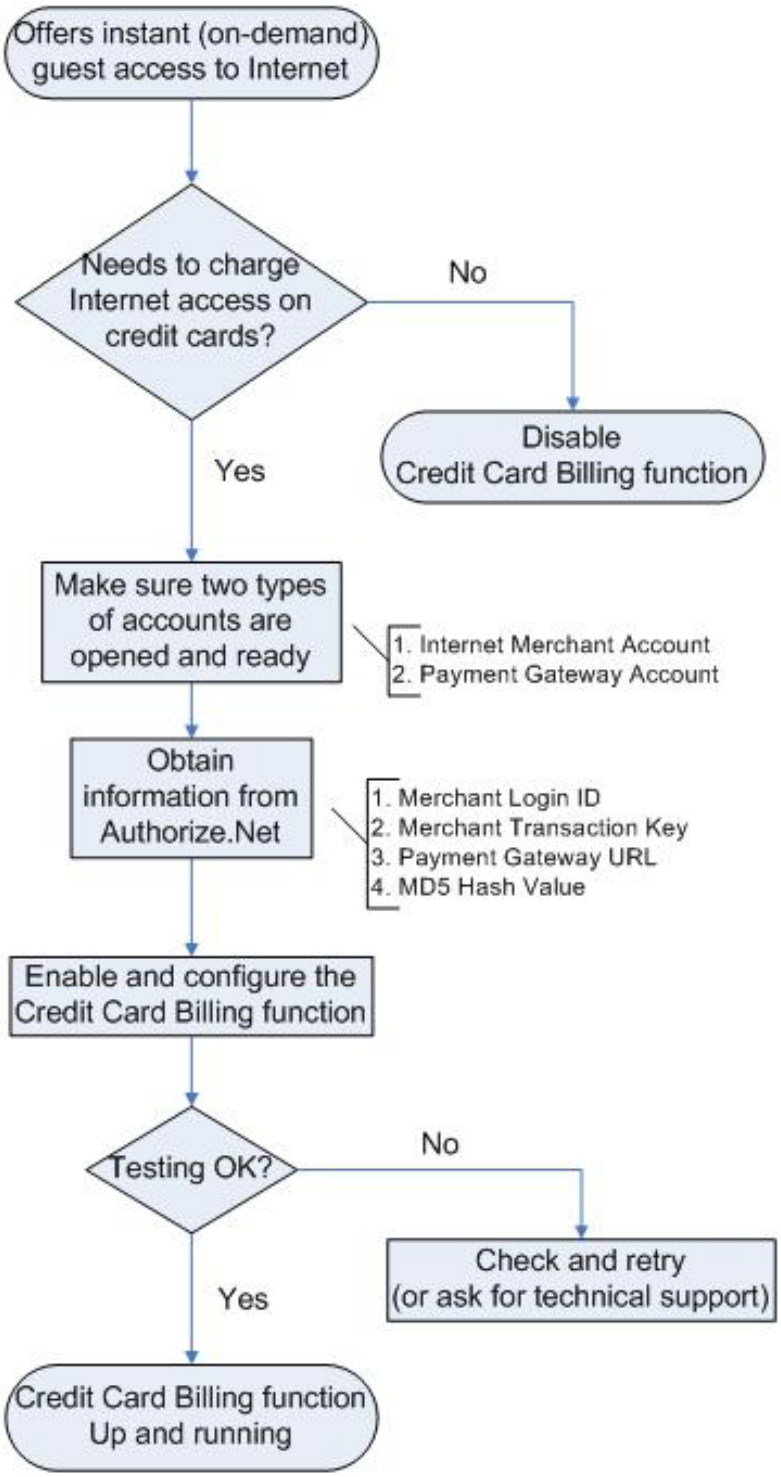
- **Report All:** Click this to get a complete report including all the on-demand records. This report shows the total expenses and individual accounting of each plan for all plans available.

Report All	
Accounts sold in total	2
Plan1	2
Plan2	0
Plan3	0
Plan4	0
Plan5	0
Plan6	0
Plan7	0
Plan8	0
Plan9	0
Plan10	0
Total income	40
Income from tickets sold for time users	40
Income from tickets sold for volume users	0

- **Search:** Select a time period to get a period report. The report tells the total expenses and individual accounting of each plan for all plans available for that period of time.

Report from 2005/06/25 ~ 2005/06/28	
Accounts sold in total	2
Plan1	2
Plan2	0
Plan3	0
Plan4	0
Plan5	0
Plan6	0
Plan7	0
Plan8	0
Plan9	0
Plan10	0
Total income	40
Income from tickets sold for time users	40
Income from tickets sold for volume users	0

Credit Card: Click this to enter the **Credit Card Configuration** page. This section is about how independent HotSpot owners can enable the credit card billing function, making the HotSpot an e-commerce environment for end users to pay for and get Internet access using their credit cards. Before the "Credit Card" and related functions can be managed appropriately, WAS-102R requires the merchant owners to have a valid **Authorize.Net** (www.authorize.net) account, since Authorize.Net is the on-line payment gateway that WAS-102R supports now. Please see ***Appendix C. The Configuration on Authorize.Net*** to setup an Aurthourize.Net account and other necessary information.


Offers instant (on-demand) guest access to Internet
Needs to charge Internet access on credit cards?
No
Disable Credit Card Billing function
Yes
Make sure two types of accounts are opened and ready
1. Internet Merchant Account
2. Payment Gateway Account
Obtain information from Authorize.Net
1. Merchant Login ID
2. Merchant Transaction Key
3. Payment Gateway URL
4. MD5 Hash Value
Enable and configure the Credit Card Billing function
Testing OK?
No
Check and retry (or ask for technical support)
Yes
Credit Card Billing function Up and running

After getting an Authorize.Net account, set the following configuration in Credit Card Configuration of WAS-102R.

- **Credit Card General Configuration**

  Credit Card Payment: Click Enable to turn on this function or click Disable to turn off this function.

- **Credit Card Payment Page Configuration**

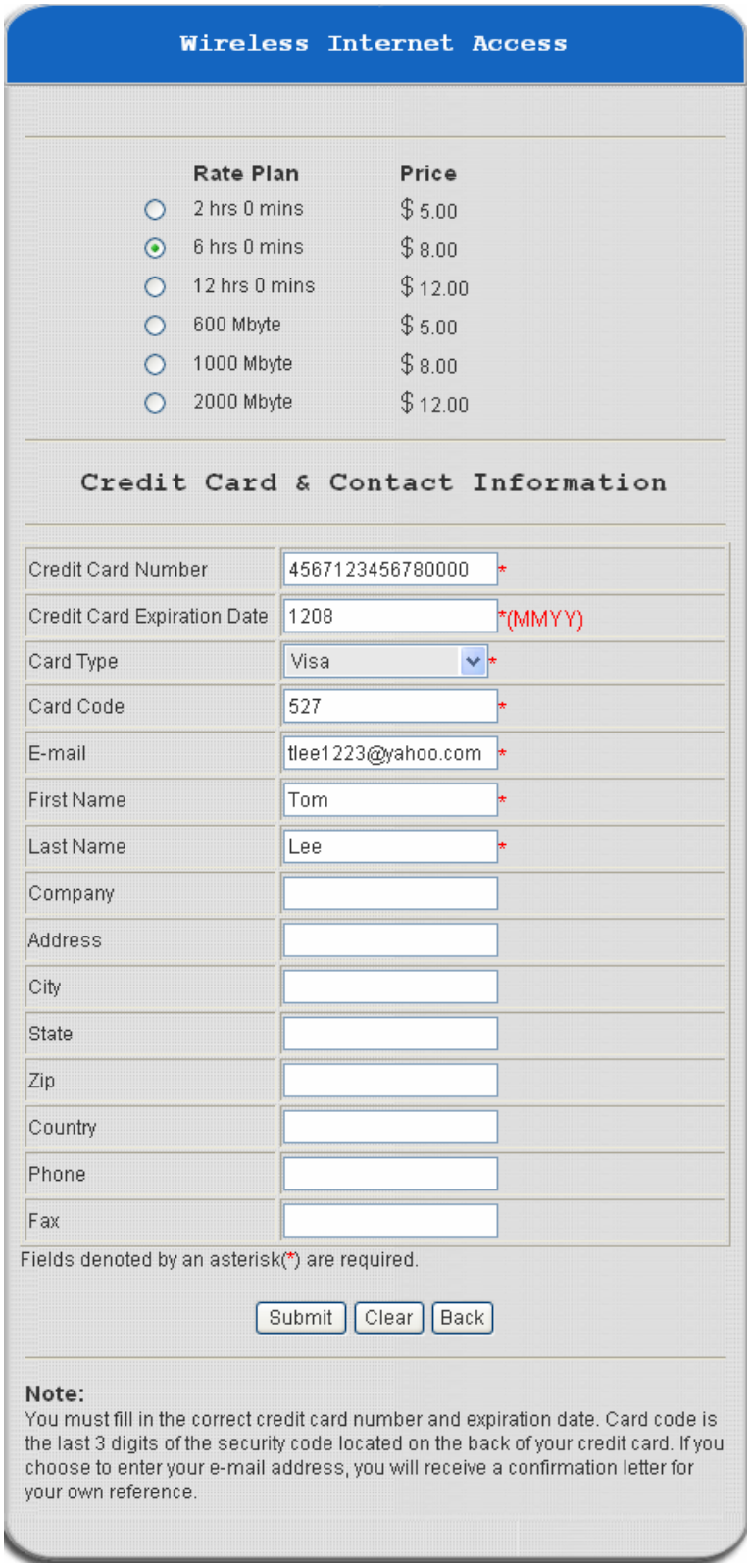
  Merchant ID: The merchant ID is similar to a username and is used by the Payment Gateway to authenticate transactions.

  Merchant Transaction Key: The merchant transaction key is similar to a password and is used by the Payment Gateway to authenticate transactions.

  Payment Gateway URL: The Payment Gateway verifies the URL specified in the post string against the URLs in this field.

  Verify SSL Certificate: ***S****ecure* ***S****ockets* ***L****ayer*, a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

Test Mode: It is possible to submit a test transactions to the payment gateway. Transactions that are submitted while Test Mode is enabled are NOT actually processed. The example as follows:

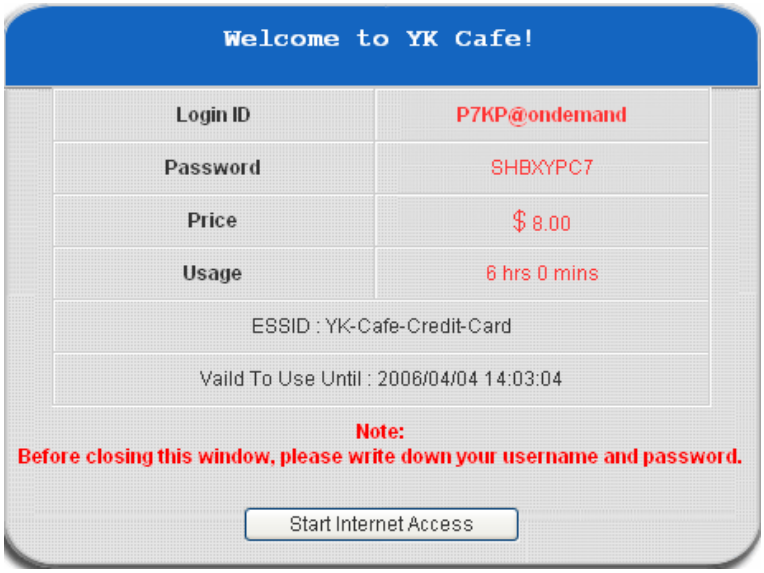


Click ***Submit*** to send out this transaction. There will be a confirm dialog box showing up. Check the data again and the click ***OK*** to go on the transaction or click ***Cancel*** to revise the data or cancel this transaction.

After clicking OK, there will be another dialog box showing up to confirm this transaction again. Click ***OK*** to complete the process or click ***Cancel*** to revise the data or cancel this transaction.

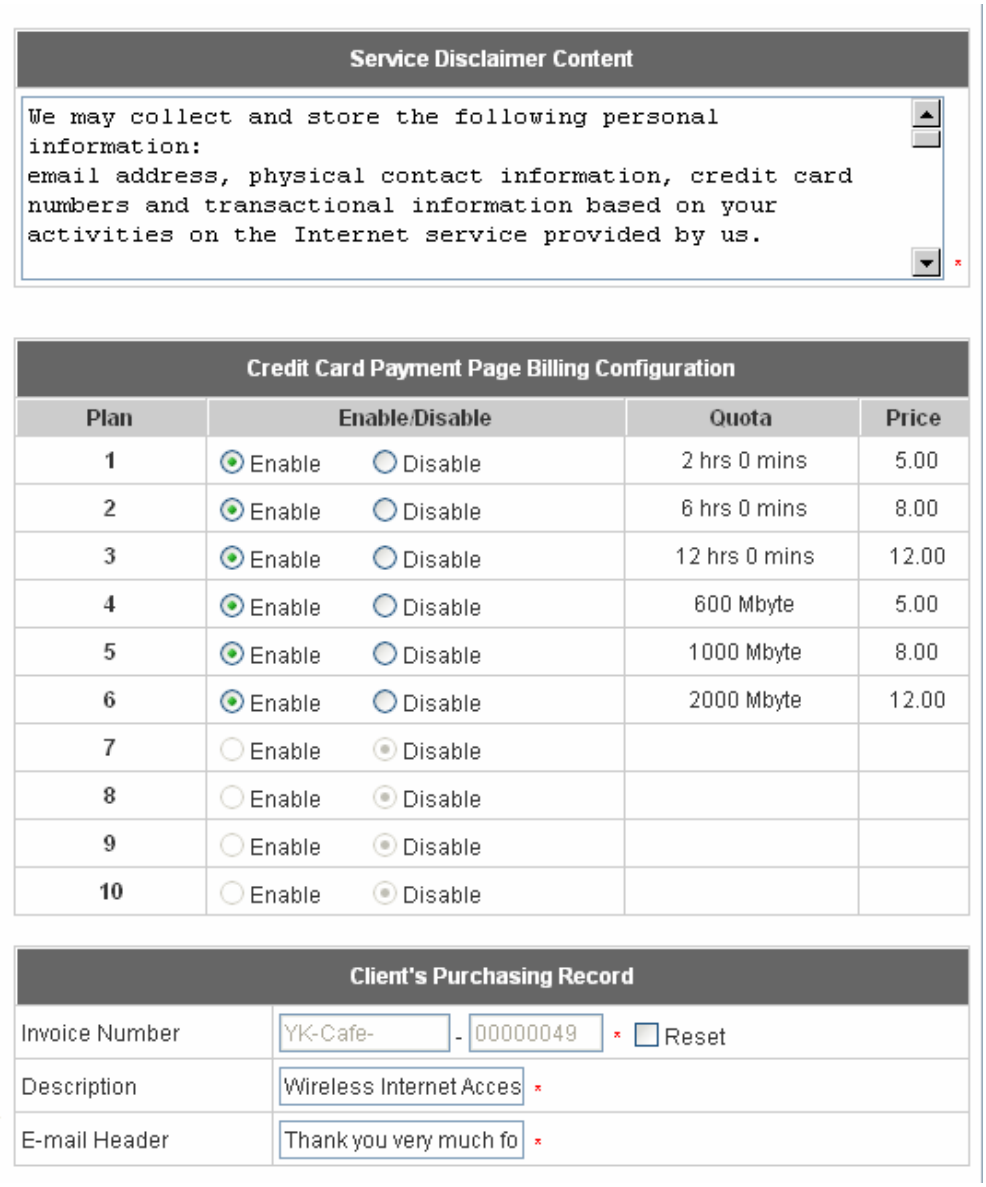
Microsoft Internet Explorer
The process may take several minnutes.
Please DO NOT close or leave this page before getting the result.
Do you want to continue the credit card payment process?
OK
Cancel

Click ***OK*** to complete the transaction and a welcome screen will show up.



Click ***Start Internet Access*** to begin to use the Internet.

MD5 Hash: If transaction responses need to be encrypted by the Payment Gateway, enter and confirm a MD5 Hash Value and select a reactive mode. The MD5 Hash security feature enables merchants to verify that the results of a transaction, or transaction response, received by their server were actually sent from the Payment Gateway.


Service Disclaimer Content
We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
Credit Card Payment Page Billing Configuration
Plan
Enable/Disable
Quota
Price
1 Enable Disable 2 hrs 0 mins 5.00
2 Enable Disable 6 hrs 0 mins 8.00
3 Enable Disable 12 hrs 0 mins 12.00
4 Enable Disable 600 Mbyte 5.00
5 Enable Disable 1000 Mbyte 8.00
6 Enable Disable 2000 Mbyte 12.00
7 Enable Disable
8 Enable Disable
9 Enable Disable
10 Enable Disable
Client's Purchasing Record
Invoice Number YK-Cafe- - 00000049 * Reset
Description Wireless Internet Acces *
E-mail Header Thank you very much fo *

- **Service Disclaimer Content**

  View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.

- **Credit Card Payment Page Billing Configuration**

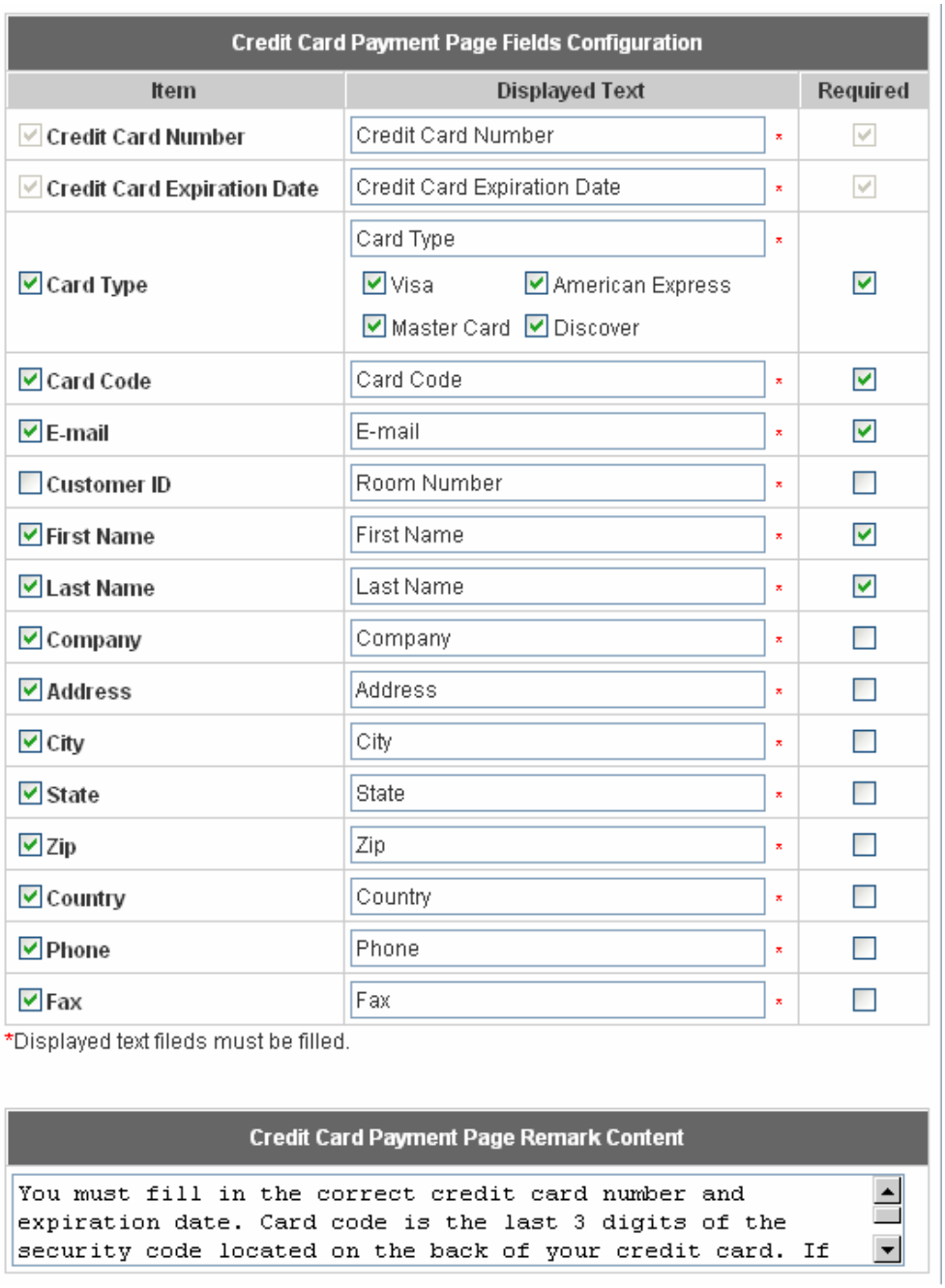
  These 10 plans are the plans in **Billing Configuration**, and desired plan can be enabled.

- **Client's Purchasing Record**

  Invoice Number: An invoice number may be provided as additional information against a transaction. This is a reference field that may contain any format of information.

  Description: Narrative text entered by a user to describe the nature of a transaction.

  Email Header: Enter the information that should appear in the header of the invoice.



Credit Card Payment Page Fields Configuration

Item	Displayed Text	Required
Credit Card Number	Credit Card Number *	
Credit Card Expiration Date	Credit Card Expiration Date *	
Card Type	Card Type * Visa American Express Master Card Discover	
Card Code	Card Code *	
E-mail	E-mail *	
Customer ID	Room Number *	
First Name	First Name *	
Last Name	Last Name *	
Company	Company *	
Address	Address *	
City	City *	
State	State *	
Zip	Zip *	
Country	Country *	
Phone	Phone *	
Fax	Fax *	

*Displayed text fileds must be filled.

Credit Card Payment Page Remark Content

You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If

- **Credit Card Payment Page Fields Configuration**

  Display: Check the box to show this item on the customer's payment interface.

  Displayed Text: Enter what needs to be shown for this field.

  Mandatory: Check the box to indicate this item as a required field.

  Credit Card Number: Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.

  Credit Card Expiration Date: Month and year expiration date of the credit card. This should be entered in the format of MMYY. For example, an expiration date of July 2005 should be entered as 0705.

Card Type: This value indicates the level of match between the Card Code entered on a transaction and the value that is on file with a customer's credit card company. A code and narrative description are provided indicating the results returned by the processor.

Card Code: The three- or four-digit code assigned to a customer's credit card number (found either on the front of the card at the end of the credit card number or on the back of the card).

Email: An email address may be provided along with the billing information of a transaction. This is the customer's email address and should contain an @ symbol.

Customer ID: This is an internal identifier for a customer that may be associated with the billing information of a transaction. This field may contain any format of information.

First Name: The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.

Last Name: The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.

Company: The name of the company associated with the billing or shipping information entered on a given transaction.

Address: The address entered either in the billing or shipping information of a given transaction.

City: The city is associated with either the billing address or shipping address of a transaction.

State: A state is associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.

Zip: The ZIP code represents the five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.

Country: The country is associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full value.

Phone: A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.

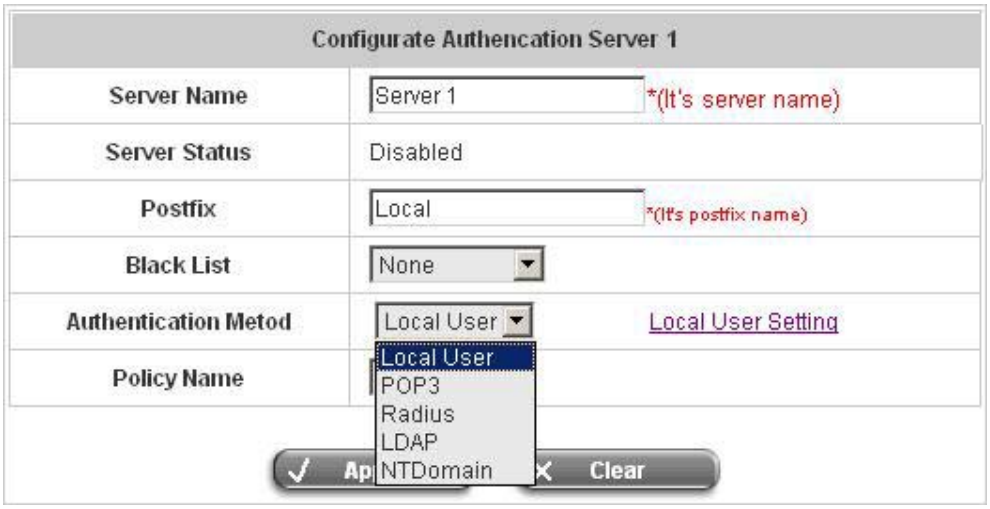
Fax: A fax number may be associated with the billing information of a transaction. This number may be entered as all number or contain parentheses and dashes to separate the area code and number.

- **Credit Card Payment Page Remark Content**

  Enter additional details for the transaction such as Tax, Freight and Duty Amounts, Tax Exempt status, and a Purchase Order Number, if applicable.

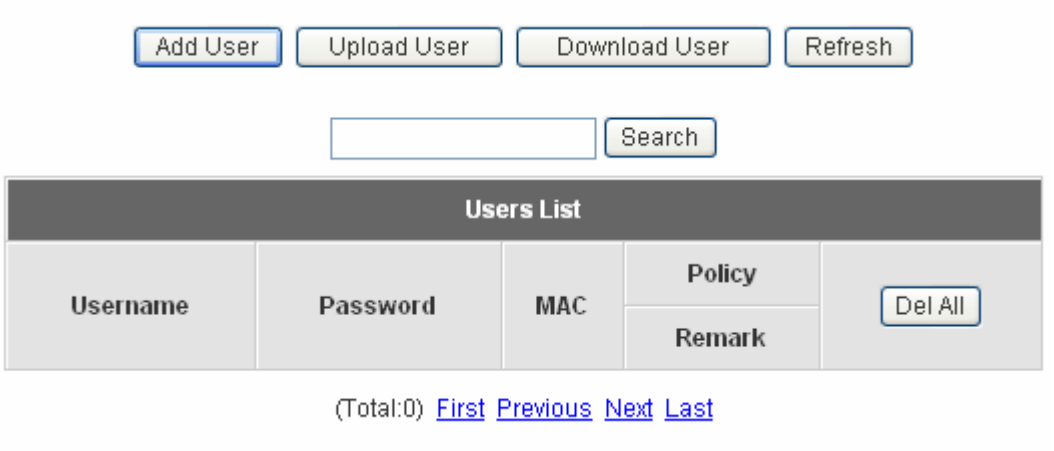
4.2.1.1 Authentication Method – Local User Setting

Choose **"Local User"** in the **Authentication Method** field, the hyperlink besides the pull-down menu will become **"Local User Setting"**.



Click the hyperlink for further configuration.

- **Edit Local User List:** Click this to enter the **"Local User List"** screen.



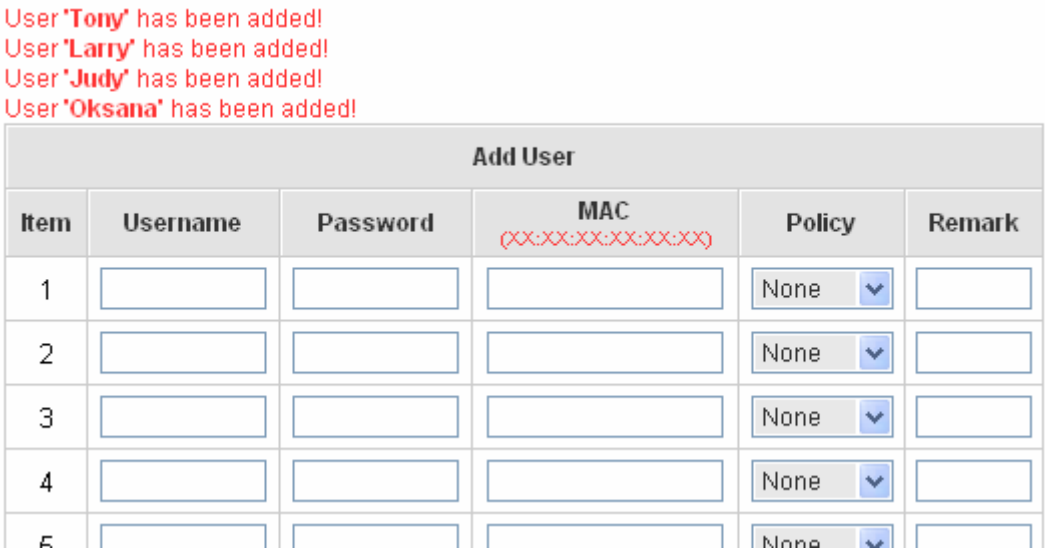
Add User: Click ***this*** to enter the **Add User** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC"** and **"Remark"** (optional). Then, select a desired **Policy** and click ***Apply*** to complete adding the user or users.

Add User					
Item	Username	Password	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
1				None	
2				None	
3				None	
4				None	
5				None	
6				None	
7				None	
8				None	
9				None	
10				None	

Input the users and enter the necessary information.

Add User					
Item	Username	Password	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
1	Tony	asti234		Policy A	
2	Larry	1deTg5	00:01:23:3F:6D:7E	Policy A	
3	Judy	fish258		None	
4	Oksana	oklova		Policy B	long term
5				None	
6				None	
7				None	
8				None	
9				None	
10				None	

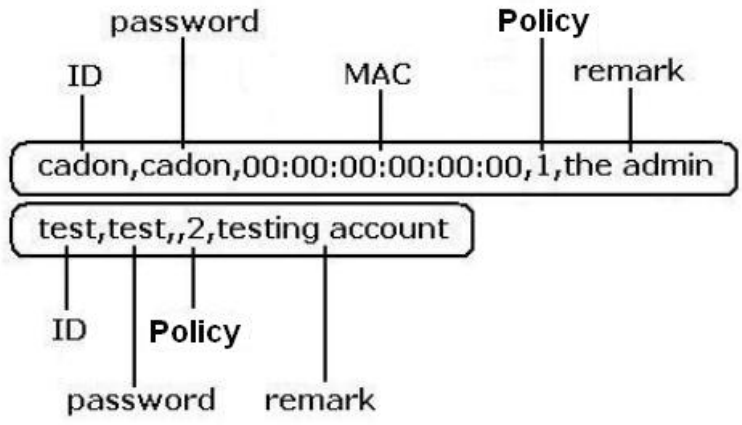
After inputting the users and all the information desired, click ***Apply***.



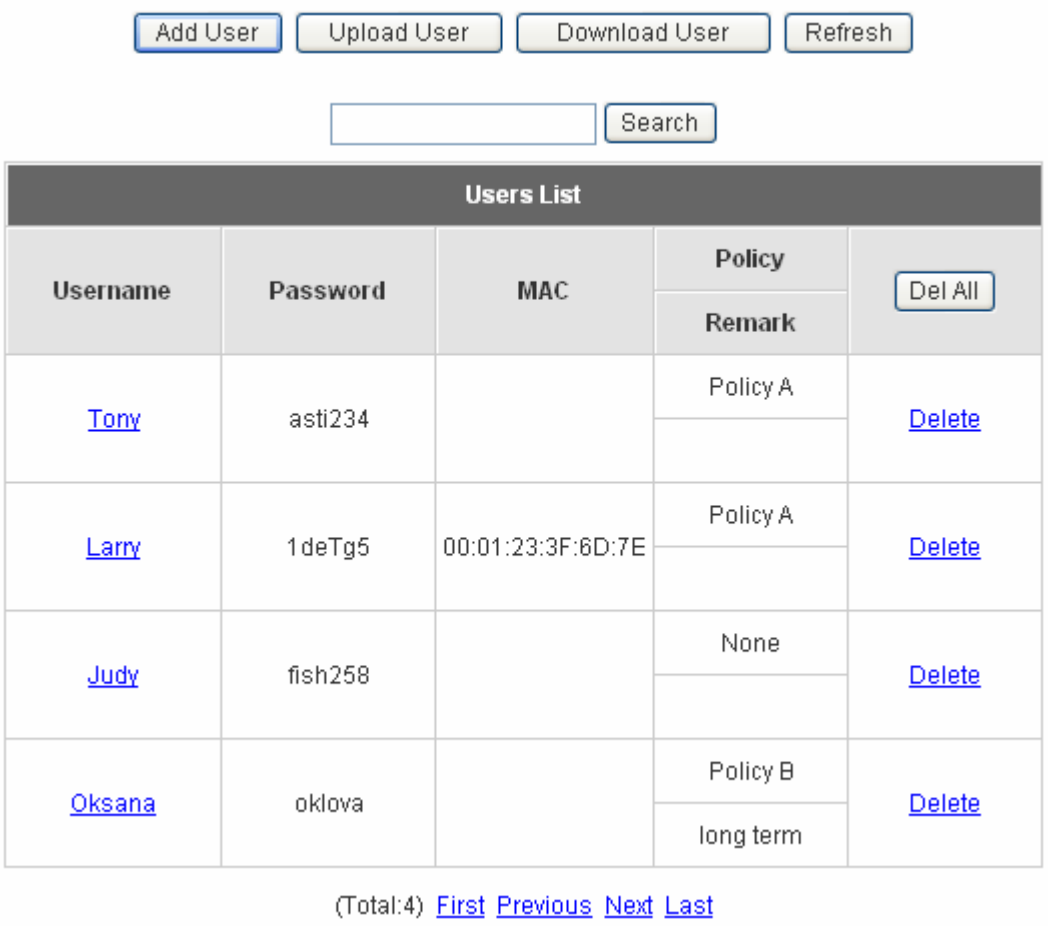
Upload User: Click this to enter the **Upload User** interface. Click the ***Browse*** button to select the text file for the user account upload. Then click ***Submit*** to complete the upload process.

Note: The format of each line is "ID, Password, MAC, Policy, Remark" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.
Upload User Account
File Name
Browse...
Submit

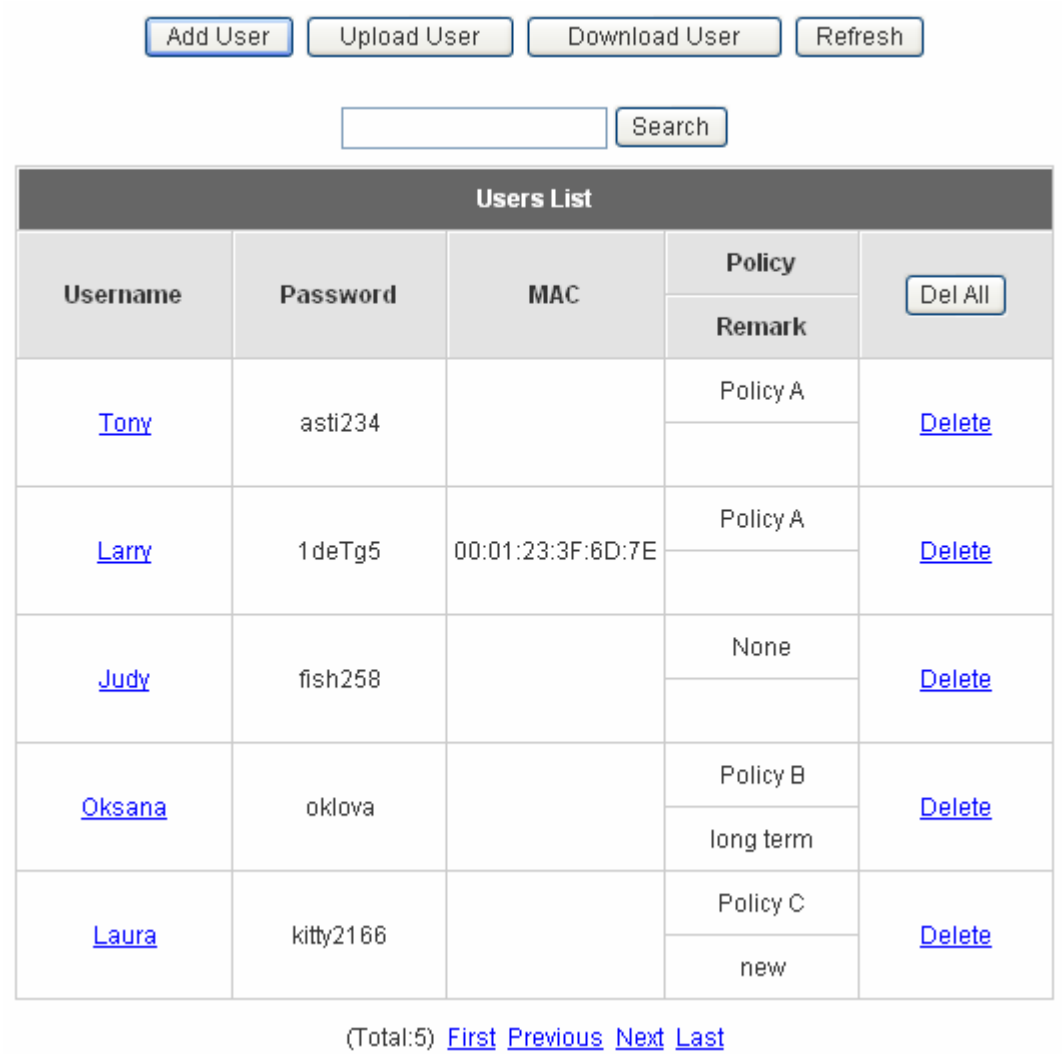
The uploading file should be a text file and the format of each line is ***"ID, Password, MAC, Policy, Remark"*** without the quotes. There must be no spaces between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by new ones.



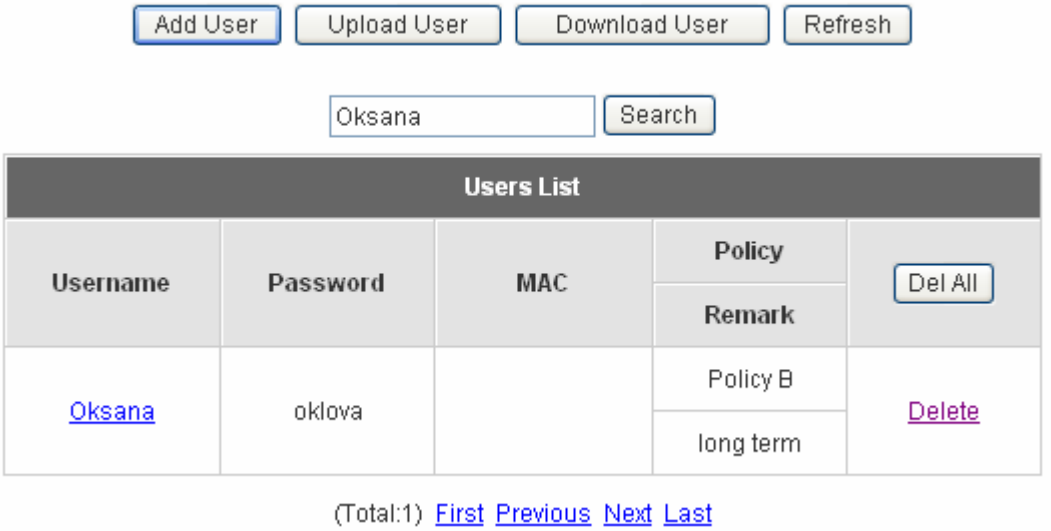
Download User: Click this to enter the **Users List** page and the system will directly show a list of all created user accounts. Click ***Download*** to create a .txt file and then save it on disk.



Refresh: Click this to renew the user list.



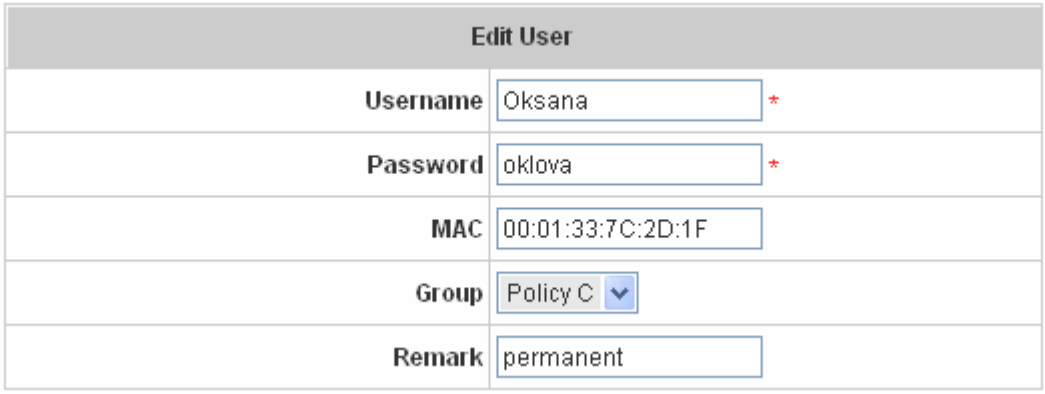
Search: Enter a keyword of a username to be searched in the text field and click this button to perform the search. All usernames matching the keyword will be listed.



Del All: This will delete all the users at once.

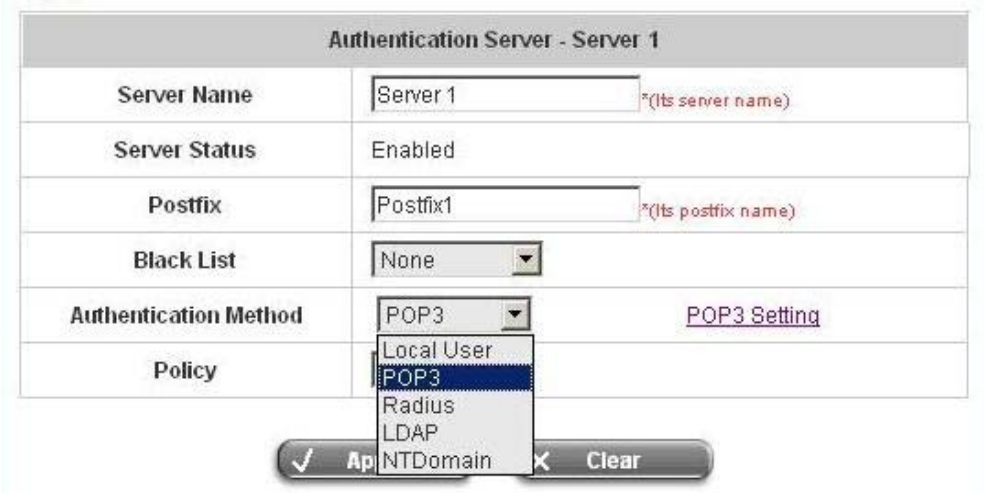
Delete: This will delete the users individually.

Edit User: If editing the content of individual user account is desired, click the username of the desired user account to enter the **Edit User** Interface for that particular user, and then modify or add any desired information such as **"Username"**, **"Password"**, **"MAC"** and **"Remark"** (optional). Then, click ***Apply*** to complete the modification.

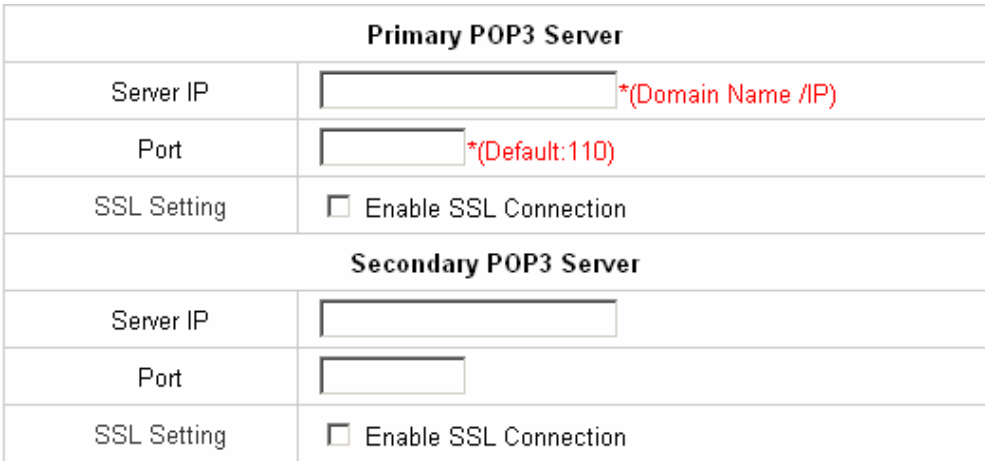


4.2.1.2 Authentication Method – POP3

Choose **"POP3"** in the **Authentication Method** field, the hyperlink beside the pull-down menu will become **"POP3 Setting"**.



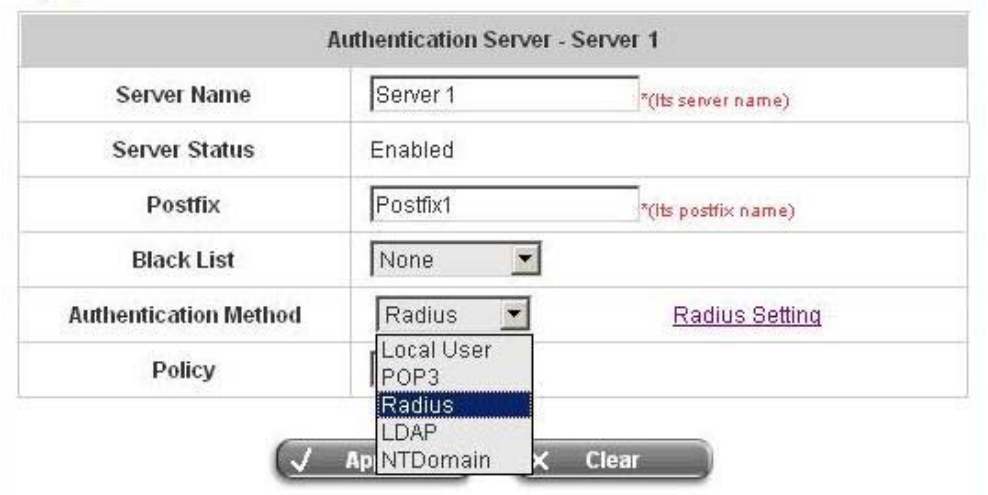
Click the hyperlink for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.



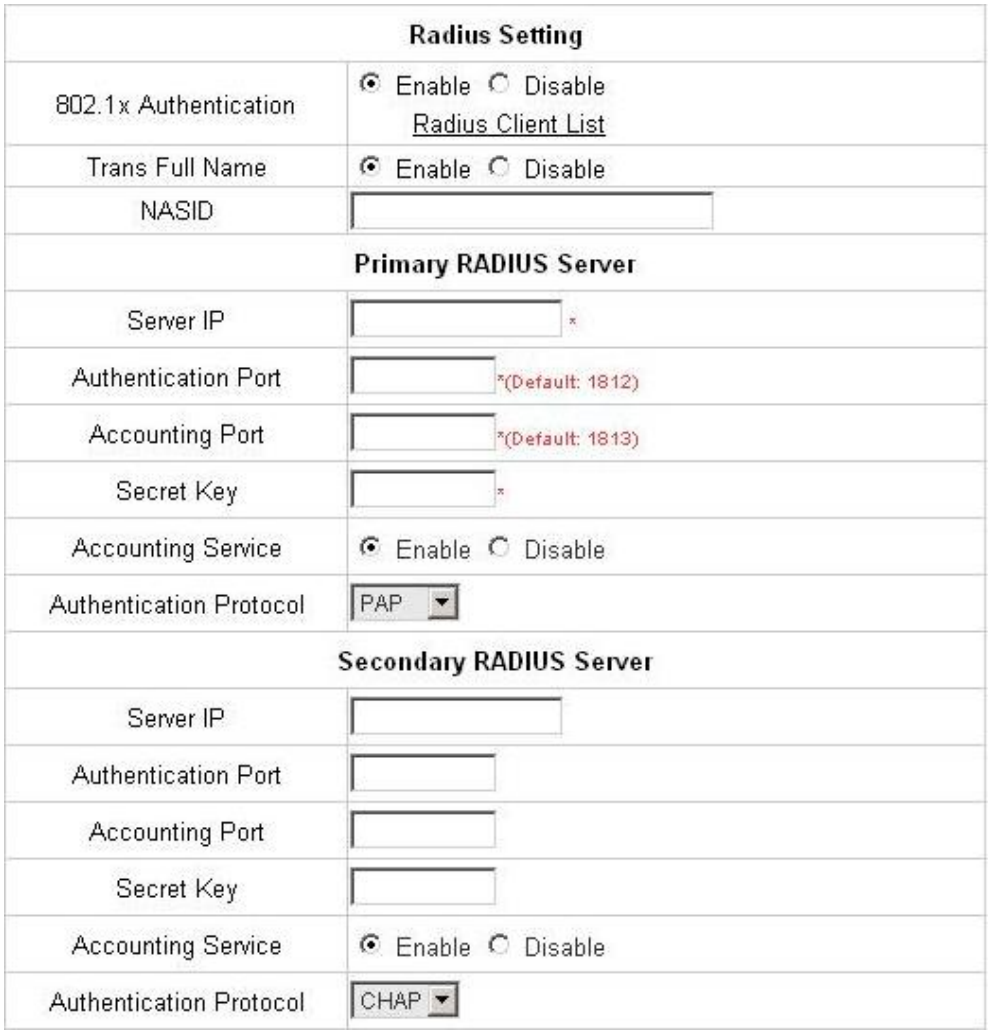
- **Server IP:** Enter the IP address/domain name given by the ISP.
- **Port:** Enter the Port given by the ISP. The default value is 100.
- **Enable SSL Connection:** If this option is enabled, the POP3 protocol will perform the authentication.

4.2.1.3 Authentication Method – Radius

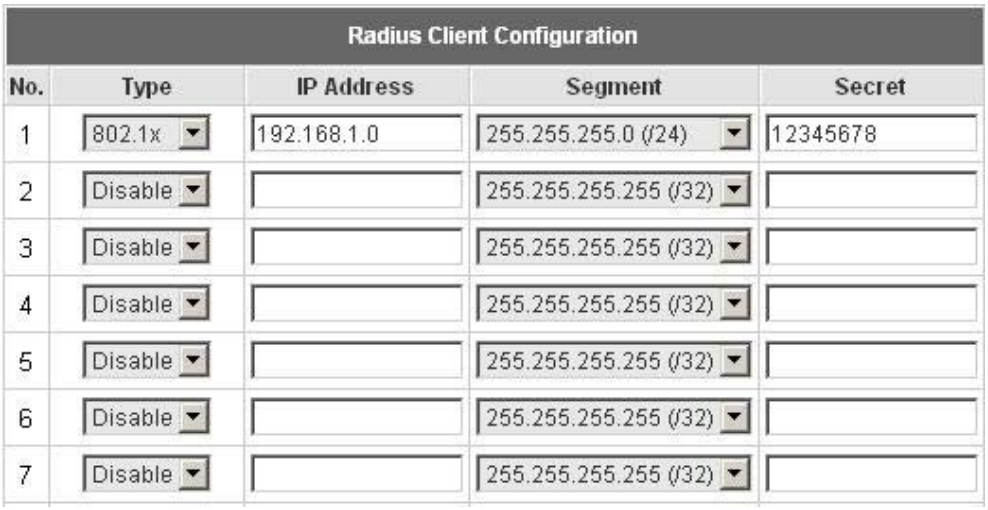
Choose **"Radius"** in the **Authentication Method** field, the hyperlink beside the pull-down menu will become **"Radius Setting"**.



Click the hyperlink for further configuration. The Radius server sets the external authentication for user accounts. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.



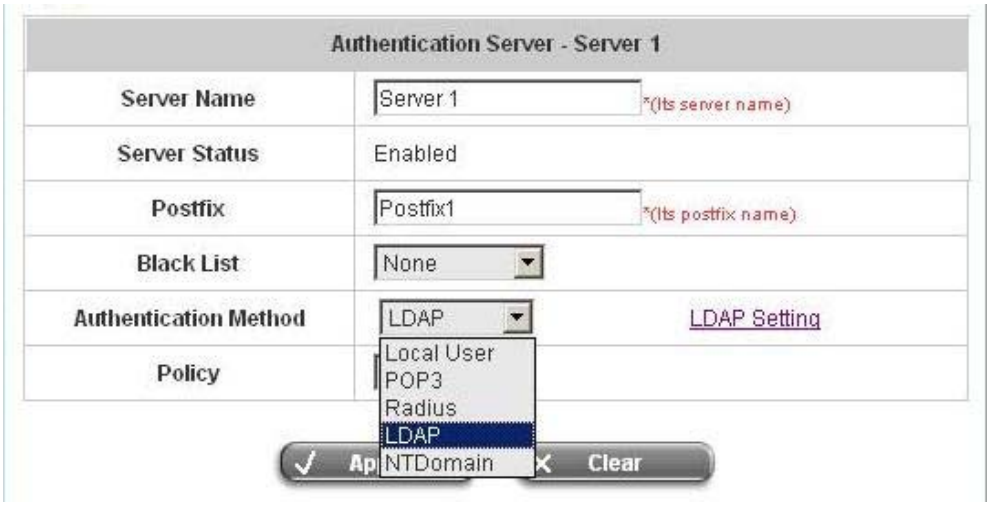
- **802.1X Authentication:** Enable this function and the hyperlink of ***Radius Client List*** will appear. Click the hyperlink to get into the Radius Client Configuration list for further configuration. In the **Radius Client Configuration** table, the clients, which are using 802.1X as the authentication method, shall be put into this table. WAS-102R will forward the authentication request from these clients to the configured Radius Servers.



- **Trans Full Name:** When enabled, the ID and postfix will be transferred to the RADIUS server for authentication. When disabled, only the ID will be transferred to RADIUS server for authentication.
- **NASID:** Enter a line of characters, for example "meeting room", for identify the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.), all other letters are not allowed.
- **Server IP:** Enter the IP address/domain name of the RADIUS server.
- **Authentication Port:** Enter the authentication port of the RADIUS server and the default value is 1812.
- **Accounting Port:** Enter the accounting port of the RADIUS server and the default value is 1813.
- **Secret Key:** Enter the key for encryption and decryption.
- **Accounting Service:** Select this to enable or disable the **"Accounting Service"** for accounting capabilities.
- **Authentication Protocol:** There are two methods, CHAP and PAP for selection.

4.2.1.4 Authentication Method – LDAP

Choose **"LDAP"** in the **Authentication Method** field, the hyperlink beside the pull-down menu will become **"LDAP Setting"**.



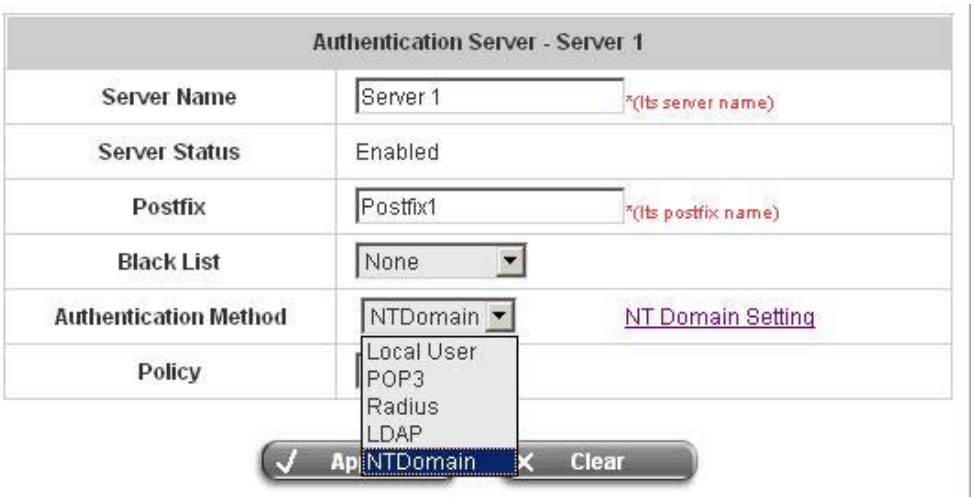
Click the hyperlink for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.

Primary LDAP Server	
Server IP	*(Domain Name/IP)
Port	*(Default:389)
Base DN	*(CN=,dc=,dc=)
Account Attribute	*(Default:uid)
Secondary LDAP Server	
Server IP	
Port	
Base DN	
Account Attribute	

- **Server IP:** Enter the IP address or domain name of the LDAP server.
- **Port:** Enter the Port of the LDAP server, and the default value is 389.
- **Base DN:** Enter the distinguished name of the LDAP server.
- **Account Attribute:** Enter the account attribute of the LDAP server.

4.2.1.5 Authentication Method – NTDomain

Choose **"NTDomain"** in the **Authentication Method** field, the hyperlink beside the pull-down menu will become **"NTDomain Setting"**.

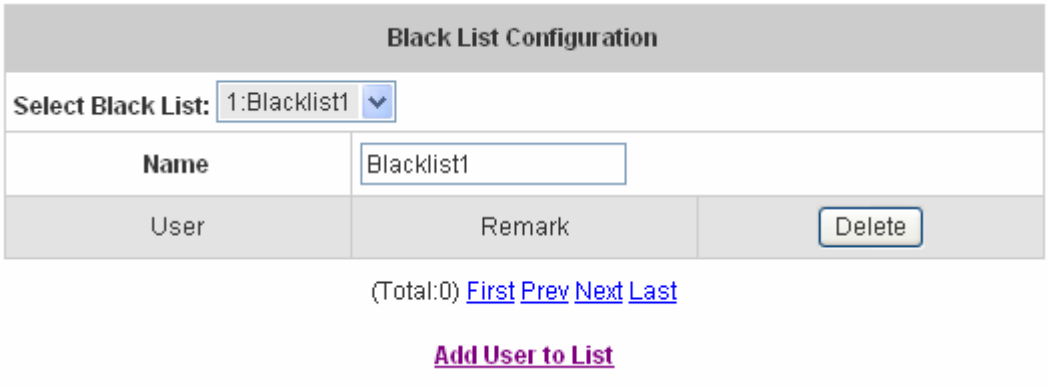


Click the hyperlink for further configuration. Enter the server IP address and enable/disable the transparent login function. These settings will become effective immediately after clicking the ***Apply*** button.

- **Server IP address:** Enter the server IP address of the domain controller.
- **Transparent Login:** If the function is enabled, users will log into WAS-102R automatically when they log into the Windows domain.

4.2.2 Black List Configuration

The administrator can add, delete, or edit the black list for user access control. Each black list can include 40 users at most. If a user in the black list wants to log into the system, the user's access will be denied. The administrator can use the pull-down menu to select the desired black list.



- **Select Black List:** There are 5 lists to select from for the desired black list.
- **Name:** Set the black list name and it will show on the pull-down menu above.

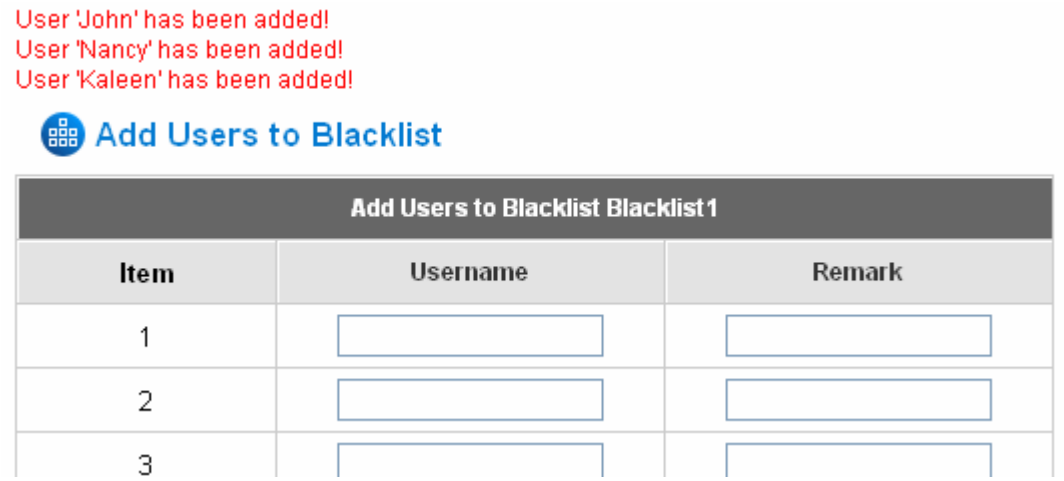
- **Add User to List:** Click the hyperlink to add users to the selected black list.

Add Users to Blacklist Blacklist1		
No	**Username**	**Remark**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

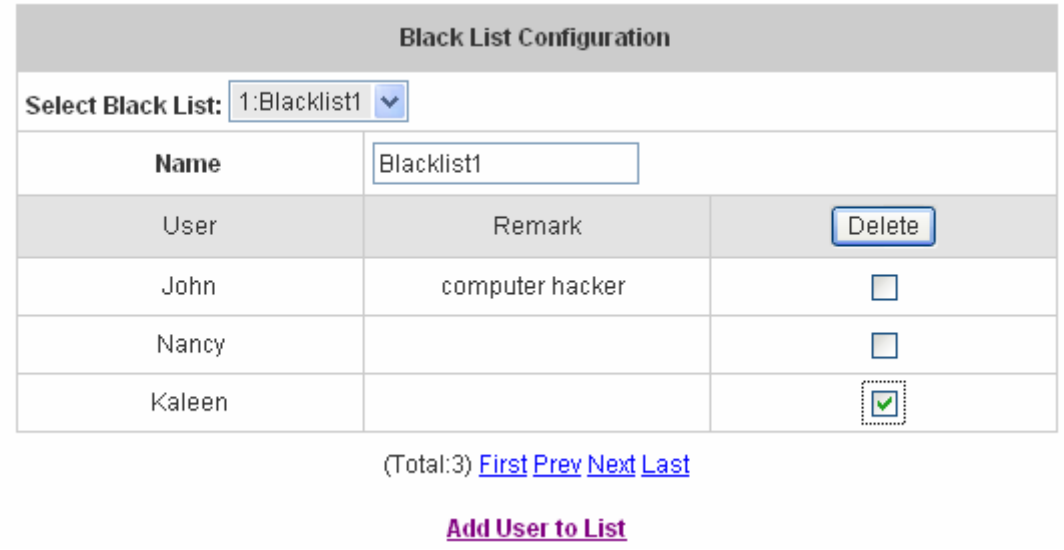
After entering the usernames in the **"Username"** blanks and the related information in the **"Remark"** blank (not required).

Add Users to Blacklist Blacklist1		
Item	**Username**	**Remark**
1	John	computer hacker
2	Nancy	
3	Kaleen	
4		
5		
6		

Click ***Apply*** to add the users.

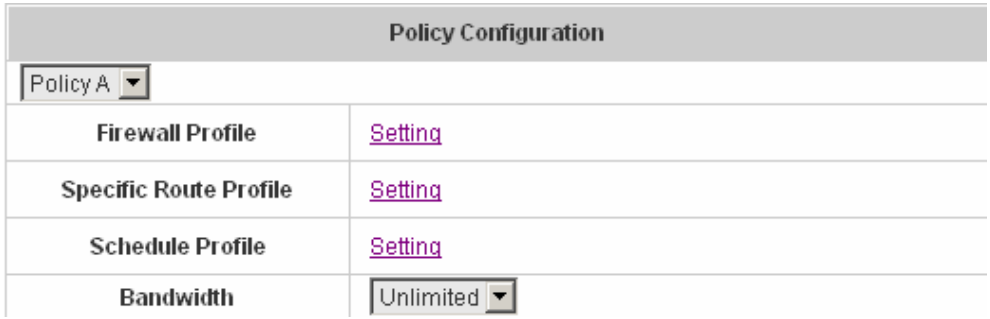


If removing a user from the black list is desired, select the user's **"Delete"** check box and then click the ***Delete*** button to remove that user from the black list.



4.2.3 Policy Configuration

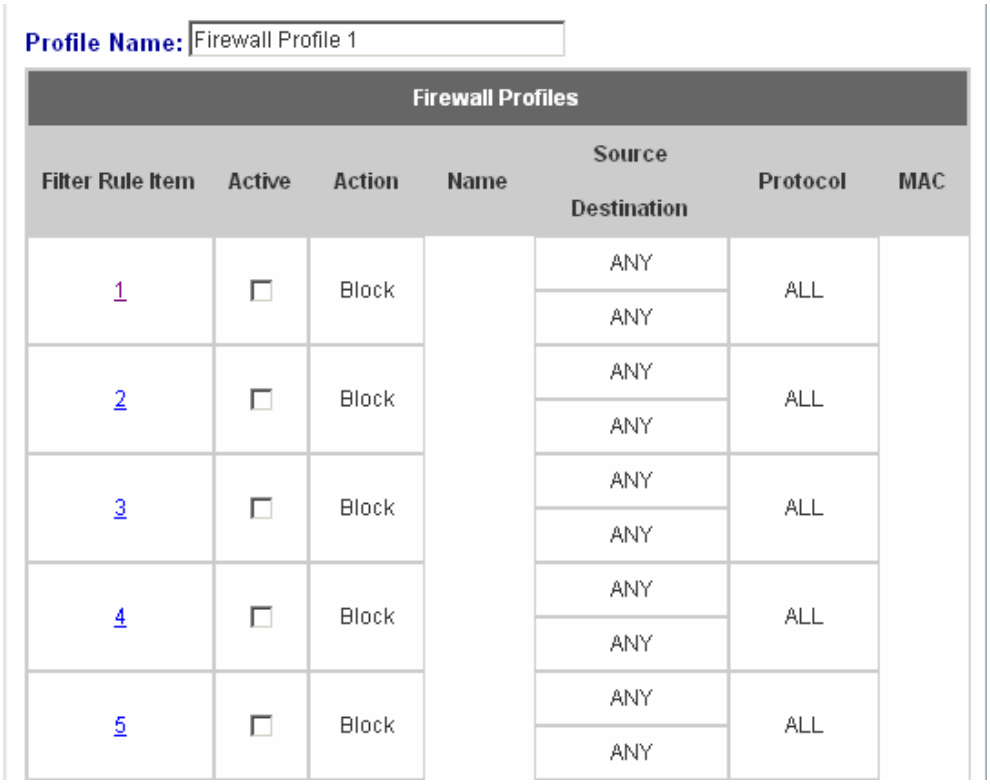
Every Policy has three profiles, **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** as well as one **Bandwidth** setting for that policy.

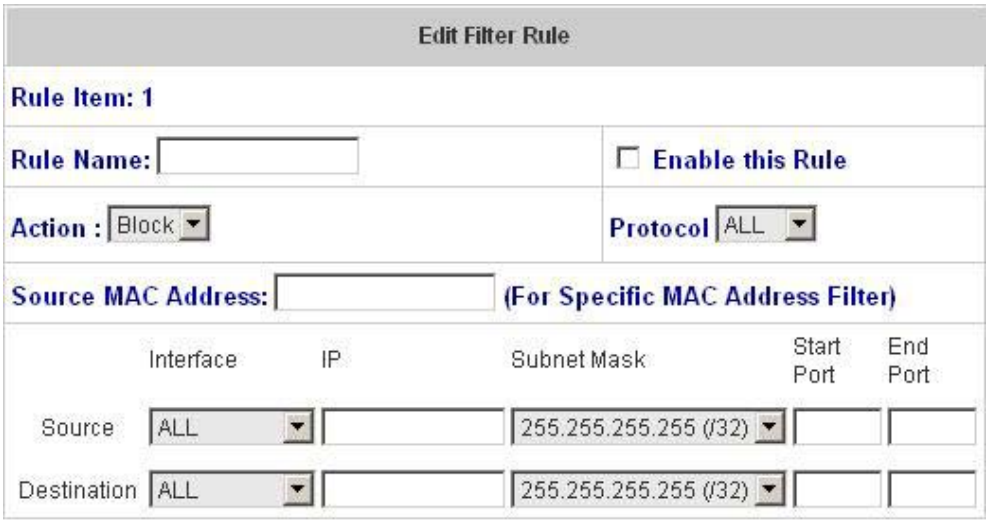


- **Firewall Profile**

  Click the hyperlink of ***Setting*** for **Firewall Profile**, the Firewall Profiles list will appear. Click the numbers of ***Filter Rule Item*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list.

Check **"Active"** to enable that rule.





Rule Item: This is the rule selected.

Rule Name: The rule name can be changed here.

Enable this Rule: After checking this function, the rule will be enabled.

Action: There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.

Protocol: There are three protocols to select, **TCP**, **UDP** and **ICMP**, or choose **ALL** to use all three protocols.

Source MAC Address: The MAC address of the source IP address. This is for specific MAC address filter.

Source/Destination Interface: There are four interfaces to choose, **WAN**, **Wireless**, **Public LAN (LAN1/LAN2)** and **Private LAN (LAN3/LAN4)**.

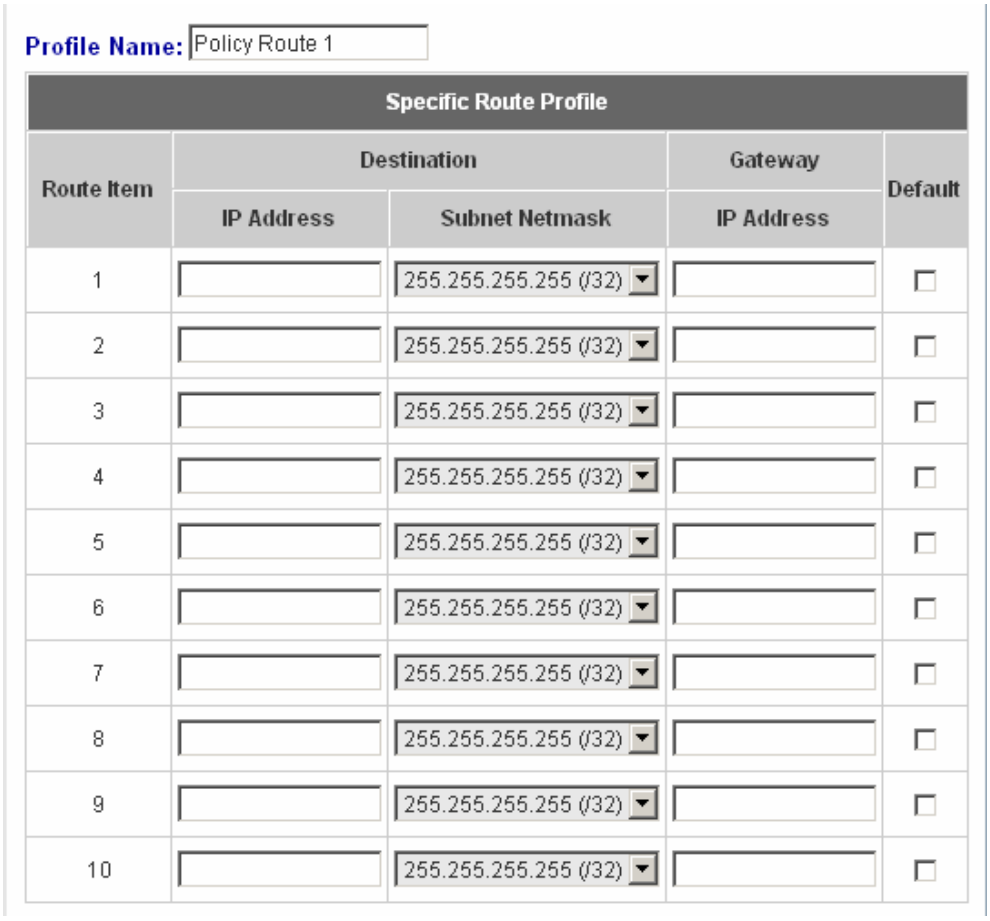
Source/Destination IP: Enter the source and destination IP addresses.

Source/Destination Subnet Mask: Enter the source and destination subnet masks.

Source/Destination Start/End Port: Enter the range of source and destination ports.

- **Specific Route Profile**

Click the hyperlink of ***Setting*** for **Specific Route Profile**, the Specific Route Profile list will appear.



Profile Name: The profile name can be changed here.

IP Address: The destination IP address of the host or the network.

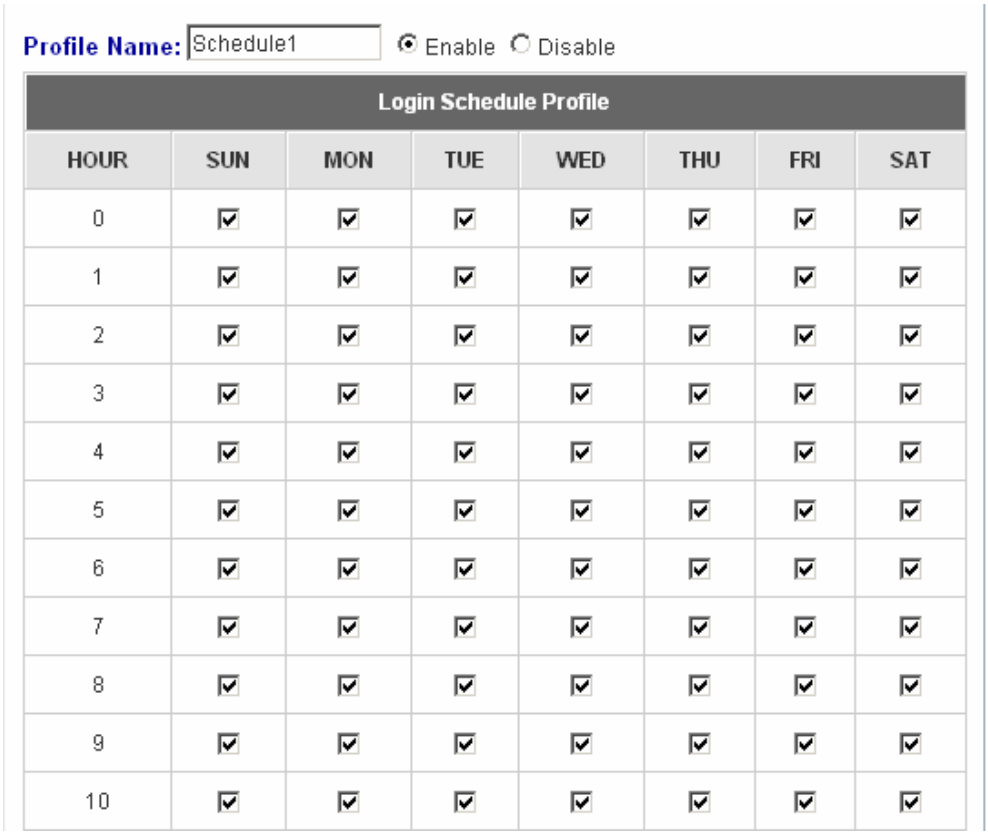
Subnet Netmask: Select a destination subnet netmask of the host or the network.

IP Address: The IP address of the next router to the destination.

Default: Check this option to apply the default value.

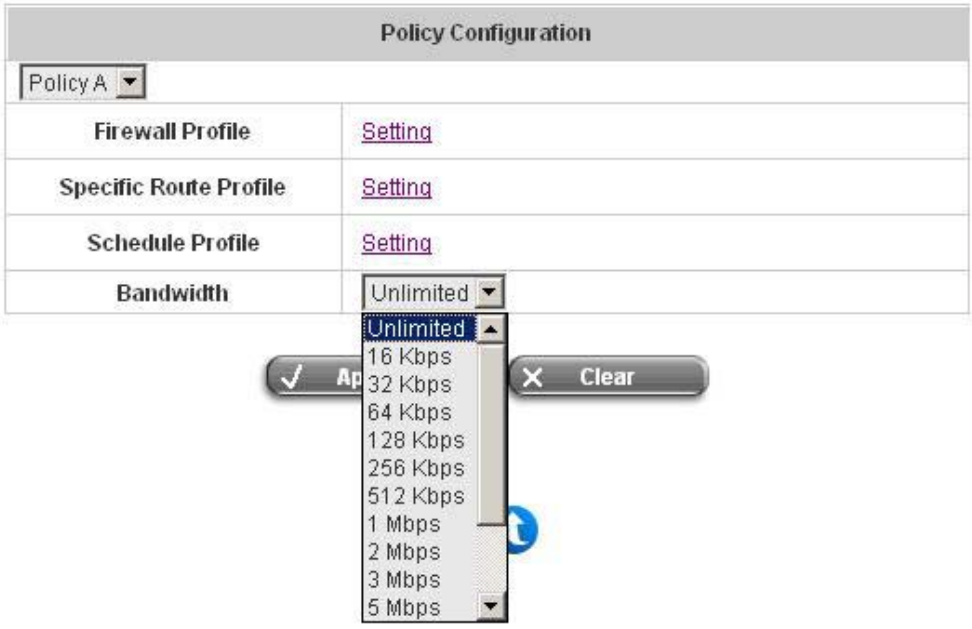
- **Schedule Profile**

Click the hyperlink of ***Setting*** for **Schedule Profile** to enter the Schedule Profile list. Select **"Enable"** to show the list. This function is used to restrict the time the users can log in. Please enable/disable the desired time slot and click ***Apply*** to save the settings. These settings will become effective immediately after clicking the ***Apply*** button.



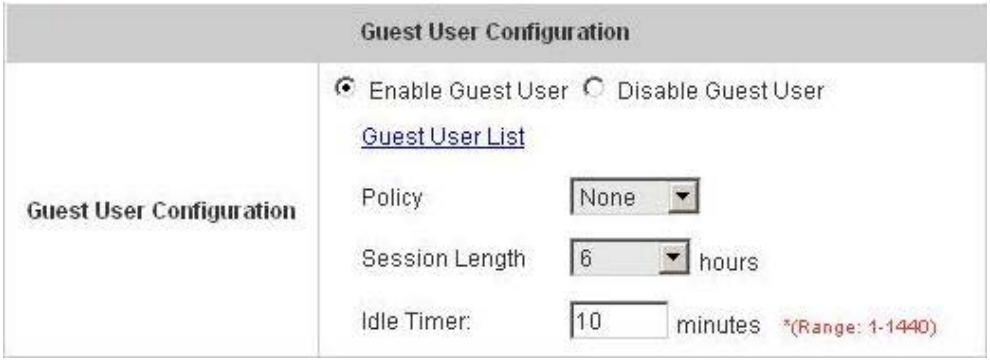
- **Bandwidth**

  Choose one bandwidth limit for that particular policy.

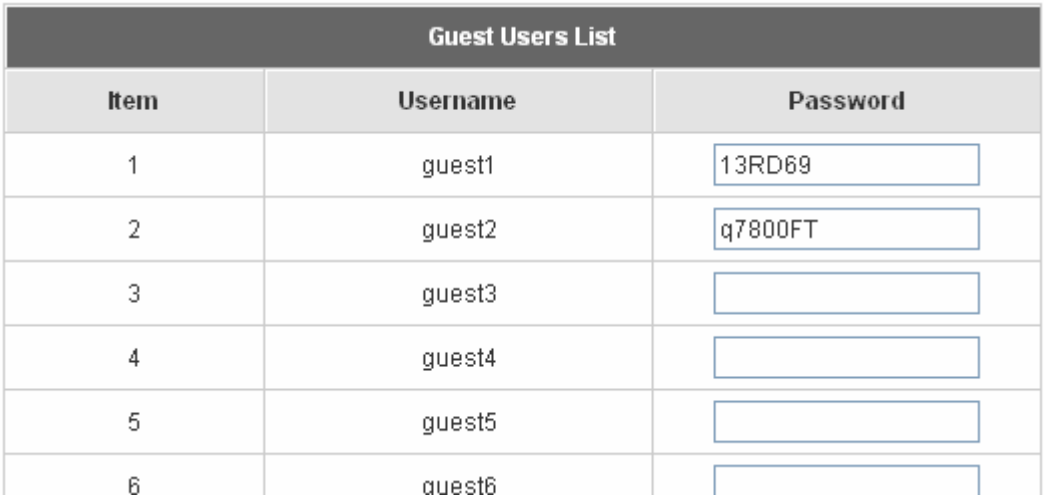


4.2.4 Guest User Configuration

This function can permit guests to log into the system. Select **"Enable Guest User"** and click ***Apply*** to save the settings.

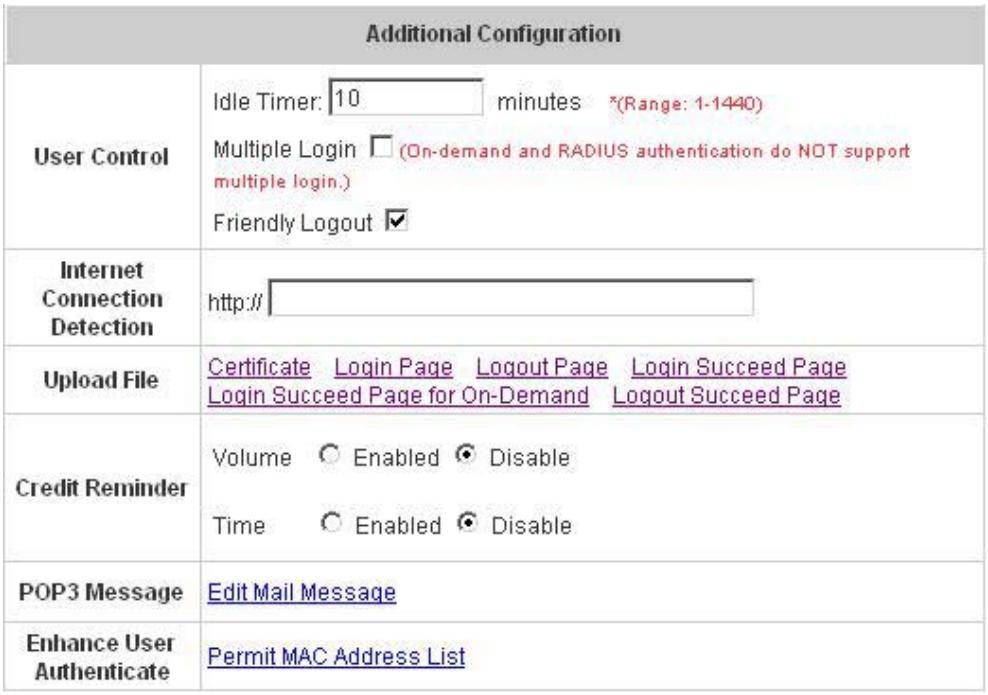


- **Guest User List:** WAS-102R offers 10 guest users for log in. To activate a guest user, just enter the password in the corresponding **"Password"** text field for that guest account. Guest accounts with blank password will not be activated.



- **Policy:** Select one policy to apply to.
- **Session Length:** This restricts the connection time of the guest users. The default session length is 6 hours and the available session time ranges from 1 to 12 hours or unlimited.
- **Idle Time:** If a user has been idled with no network activities, the system will automatically kick out the user. The logout timer can be set in the range of 1~1440 minutes, and the default logout time is 10 minutes.

4.2.5 Additional Configuration



- **User Control:** Functions under this section applies for all general users.
  Idle Timer: If a user has been idled with no network activities, the system will automatically kick out the user. The logout timer can be set in the range of 1~1440 minutes, and the default logout time is 10 minutes.
  Multiple Login: When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS accounting.)
  Friendly Logout: When a user logs into the network with wireless connection, a small window will appear to show the user's information and there is a logout button for the logout. If enabled. When the users try to close the small window, there will be a new popup window to confirm the logout in case the users click the logout button by accident.
- **Internet Connection Detection:** Enter a specific URL or IP address and WAS-102R will try to detect the network connection by sending packets directly to that specific URL or IP address. If there is a problem in the connection of the WAN port of the system such that the URL or IP address specified cannot be reached, there will be a connection failed message showing on the users' login screen.

- **Upload File**

1. **Certification:** The administrator can upload new private key and customer certification. Click the ***Browse*** button to select the file for the certificate upload. Then click ***Submit*** to complete the upload process.

Click ***Use Default Certificate*** to use the default certificate and key.

2. **Login Page:** The administrator can use the default login page or get the customized login page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click ***Preview*** to see the login page.

   a. Choose ***Default Page*** to use the default login page.

b. Choose ***Template Page*** to make a customized login page here. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.

Login Page Selection for Users	
○ Default Page	◉ Template Page
○ Uploaded Page	○ External Page

Template Page Setting	
Color for Title Background	Select (RGB values in hex mode)
Color for Title Text	Select (RGB values in hex mode)
Color for Page Background	Select (RGB values in hex mode)
Color for Page Text	Select (RGB values in hex mode)
Title	User Login Page
Welcome	Welcome To User Login Page
Information	Please Enter Your Name and Password to Sign In
Username	Username
Password	Password
Submit	Submit
Clear	Clear
Remaining	Remaining
Copyright	Copyright (c)
Preview	

c. Choose ***Uploaded Page*** to upload new login page. Click the ***Browse*** button to select the file for the login page upload. Then click ***Submit*** to complete the upload process.

After the upload process is completed, the new login page can be previewed by clicking ***Preview*** button at the bottom.

The user-defined login page must include the following HTML codes to provide the necessary fields for username and password.

```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

If the user-defined login page includes an image file, the image file path in the HTML code must be the image file to be uploaded.

```
<img src="images/xx.jpg">
```

Then, enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login page, click the ***Use Default Page*** button to restore it to default.

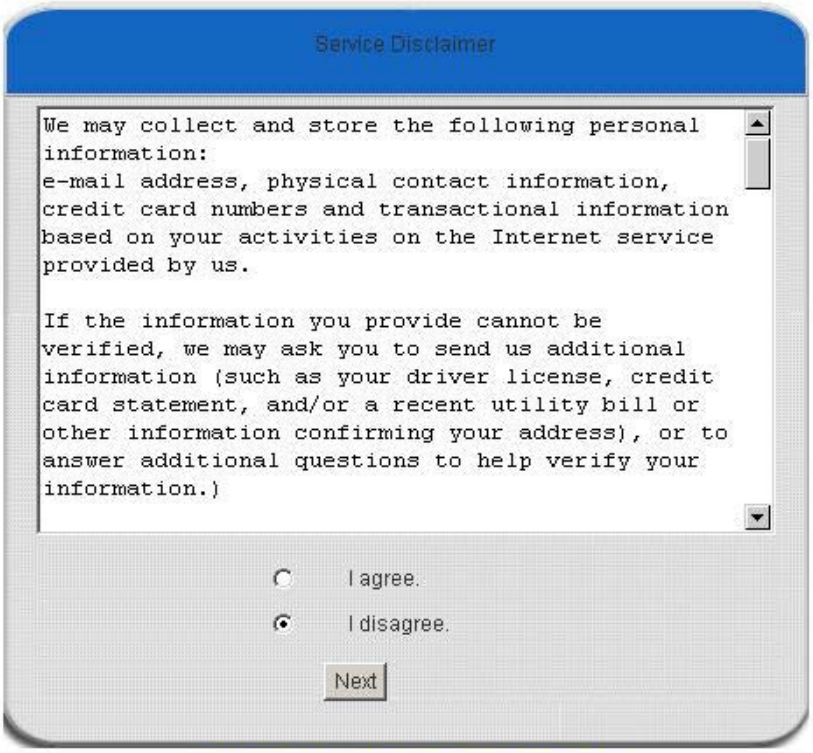
After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.

In WAS-102R, the end user first gets a login page when she/he opens its web browser right after associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display "terms of use" or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking I agree, users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

For more details about the codes of the disclaimer, please refer to Appendix E.

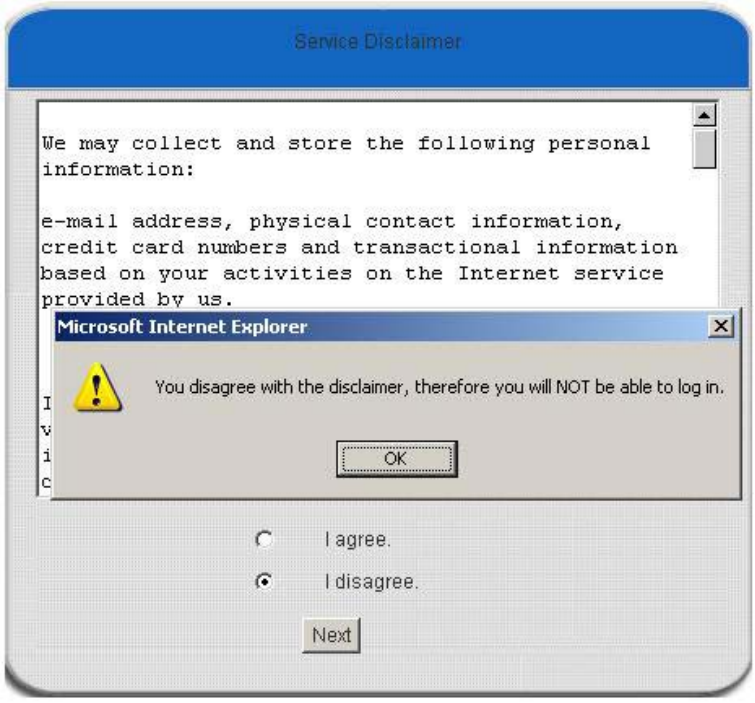
If the page is successfully loaded, an **upload success** page will show up.

"Preview" can be clicked to see the uploaded page.

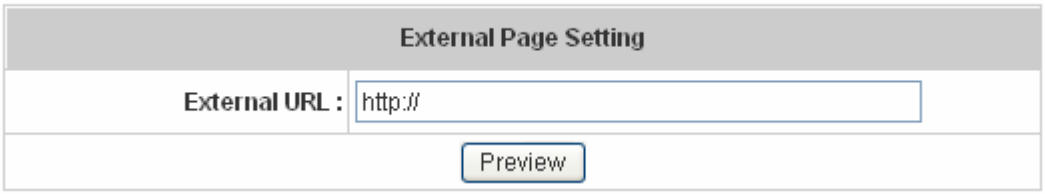

Service Disclaimer
We may collect and store the following personal information:
e-mail address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)
I agree.
I disagree.
Next
Click here to purchase by Credit Card Online.

If user checks **"I agree"** and clicks ***Next***, then he/she is prompted to fill in the login name and password.

If user checks **"I disagree"** and clicks ***Next***, a window will pop up to tell user that he/she cannot log in


Service Disclaimer
We may collect and store the following personal information:
e-mail address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
Microsoft Internet Explorer
You disagree with the disclaimer, therefore you will NOT be able to log in.
OK
I agree.
I disagree.
Next

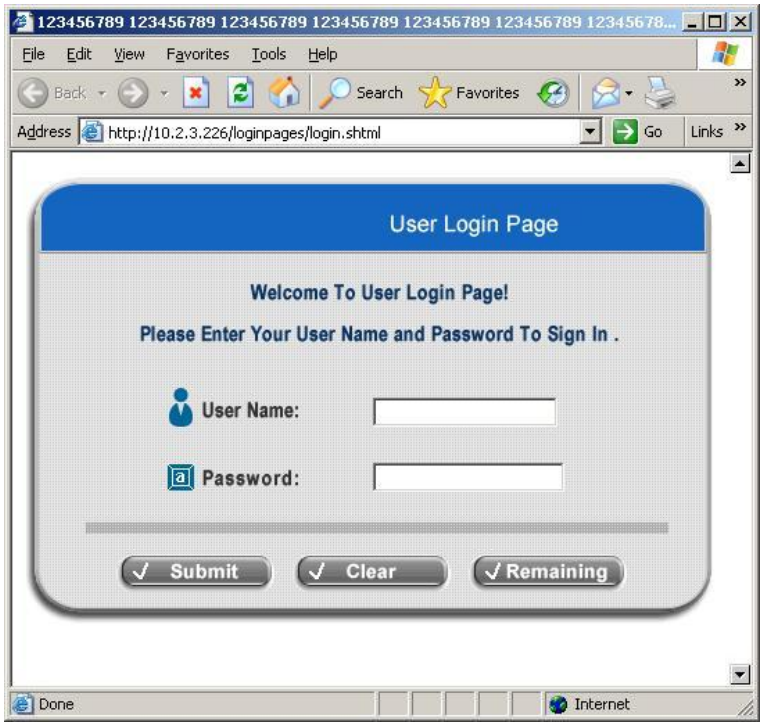
d. Choose the ***External Page*** selection and get the login page from the specific website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***.



The **External Page** prepared to be loaded here needs to have the following code as well to let the system work properly

```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

After applying the setting, the new login page can be previewed by clicking ***Preview*** button at the bottom of this page.



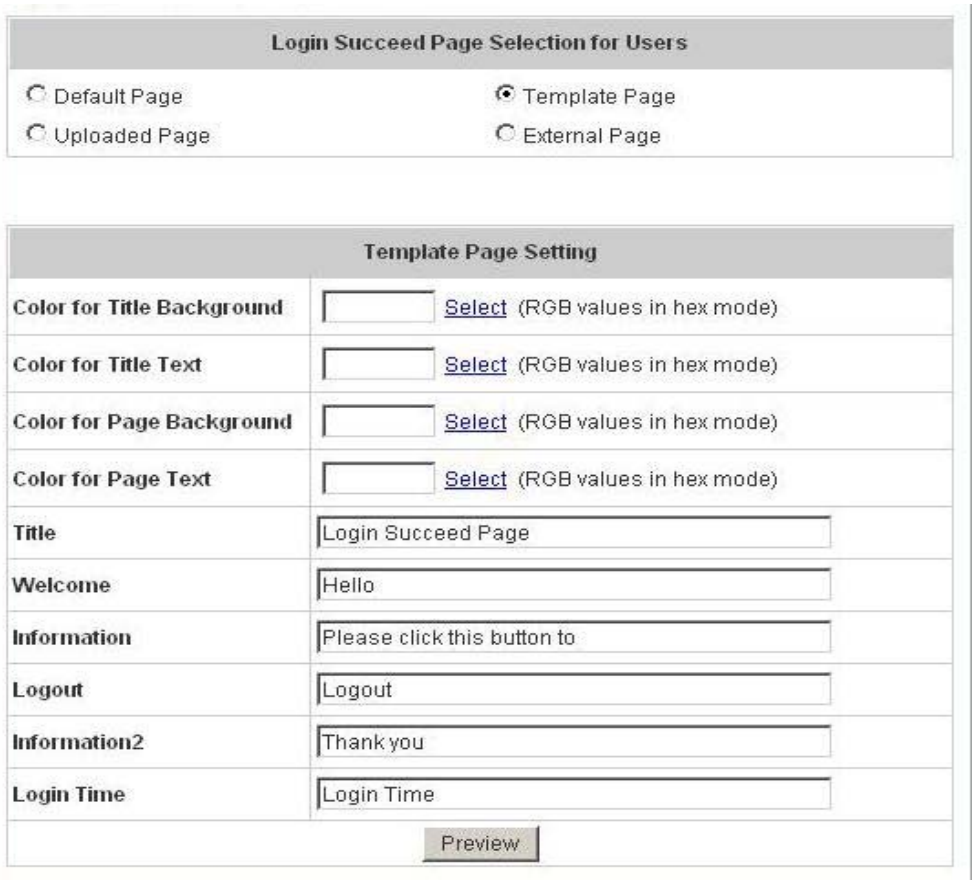
3. **Logout Page:** The users can apply their own logout page here. The process is similar to that of Logout Page.

The different part is the HTML code of the user-defined logout interface must include the following HTML

code that the user can enter the username and password. After the upload is completed, the user-defined login user interface can be previewed by clicking ***Preview*** at the bottom of this page. If want to restore the factory default setting of the logout interface, click the "**Use Default Page"** button.

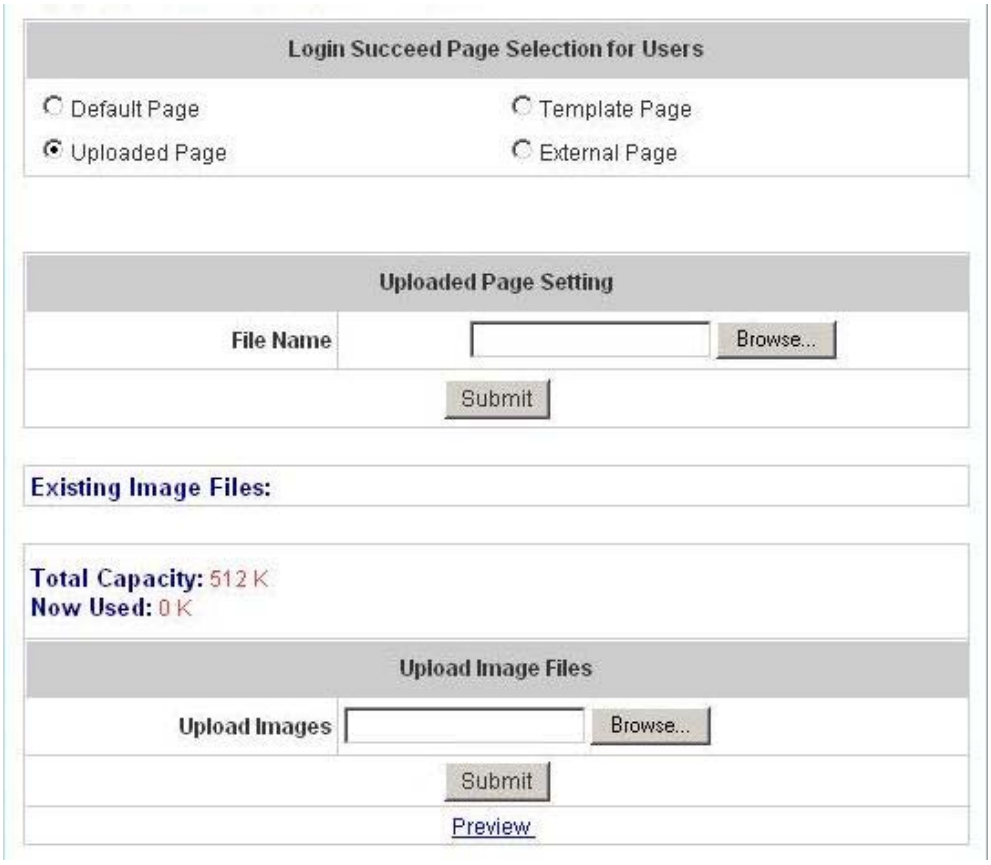
4. **Login Succeed Page:** The administrator can use the default login succeed page or get the customized login succeed page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click ***Preview*** to see the login succeed page.
   a. Choose ***Default Page*** to use the default login succeed page.

   b. Choose ***Template Page*** to make a customized login succeed page here. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



   c. Choose ***Uploaded Page*** and upload the login succeed page. Click the ***Browse*** button to select the file

for the login succeed page upload. Then click ***Submit*** to complete the upload process.

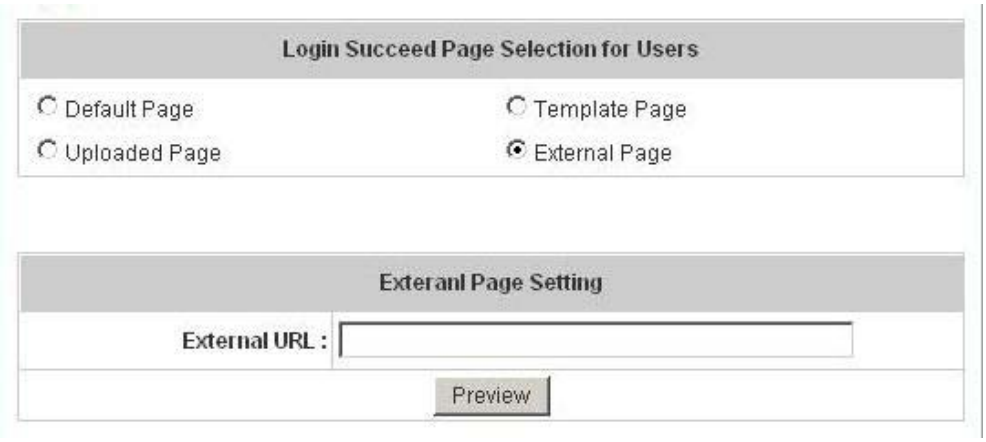


After the upload process is completed, the new login succeed page can be previewed by clicking ***Preview*** button at the bottom.

Enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login succeed page, click the ***Use Default Page*** button to restore it to default.

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.

d. Choose the ***External Page*** selection and get the login succeed page from the specific website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***. After applying the setting, the new login succeed page can be previewed by clicking ***Preview*** button at the bottom of this page.

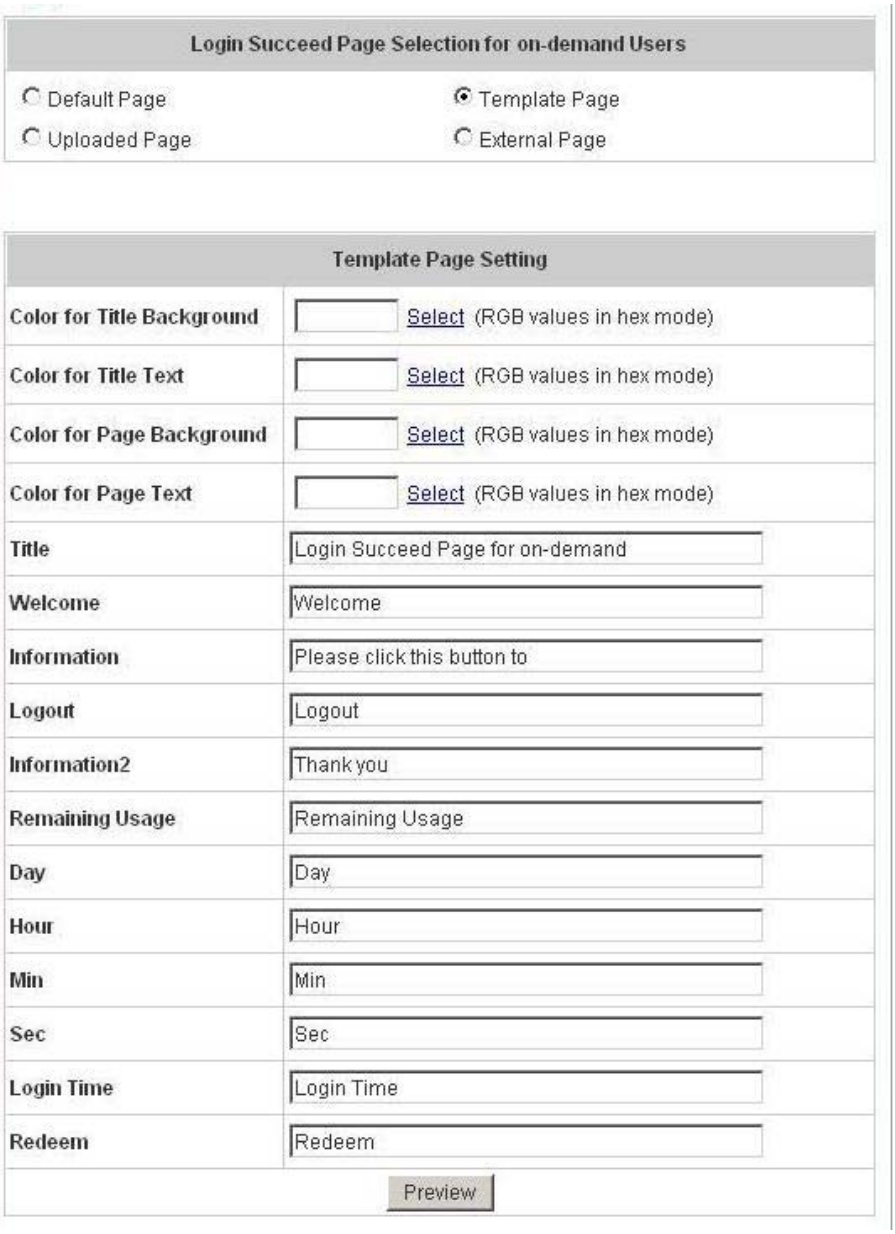


5. **Login Succeed Page for On-Demand:** The administrator can use the default login succeed page for On-Demand or get the customized login succeed page for On-Demand by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click ***Preview*** to see the login succeed page for On-Demand.

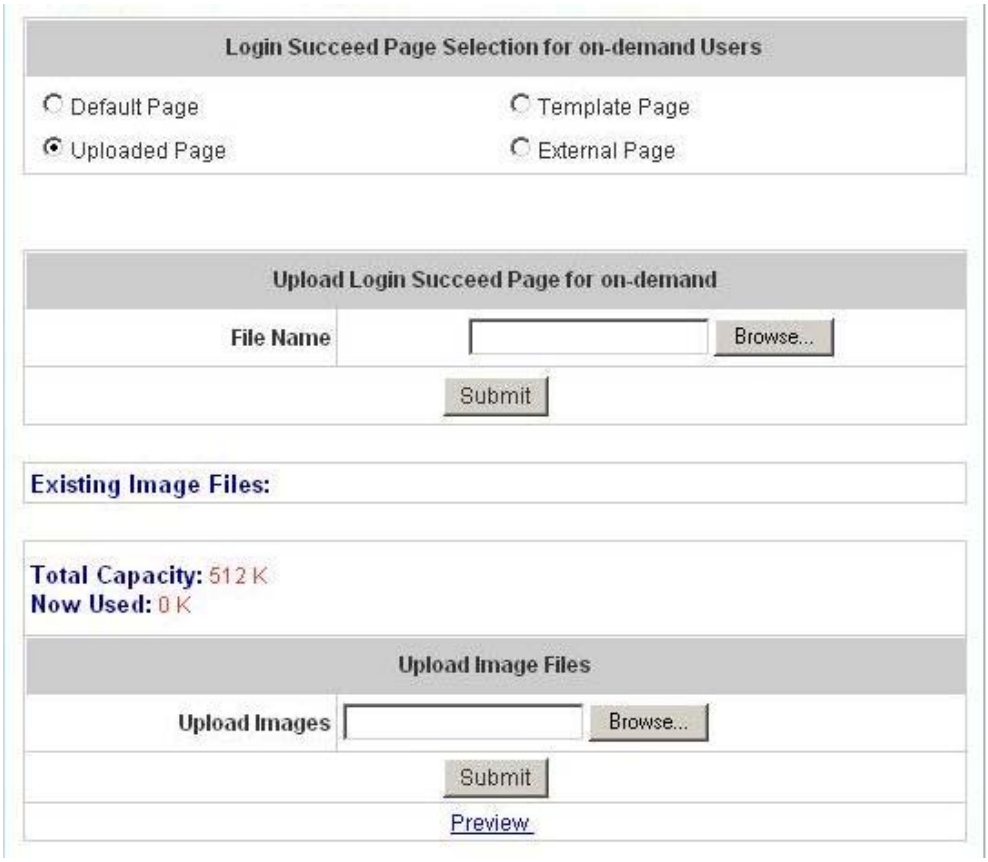
a. Choose ***Default Page*** to use the default login succeed page for On-Demand.

Login Succeed Page Selection for on-demand Users
Default Page
Template Page
Uploaded Page
External Page
Default Page Setting
This is default succeed login page for on-demand users.
You could click preview link to preview the default succeed login page.
Thanks.
Preview

b. Choose ***Template Page*** to make a customized login succeed page for On-Demand here. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



c. Choose ***Uploaded Page*** and click the ***Browse*** button to select the file for the login succeed page for On-Demand upload. Then click ***Submit*** to complete the upload process.



After the upload process is completed, the new login succeed page for On-Demand can be previewed by clicking ***Preview*** button at the bottom.

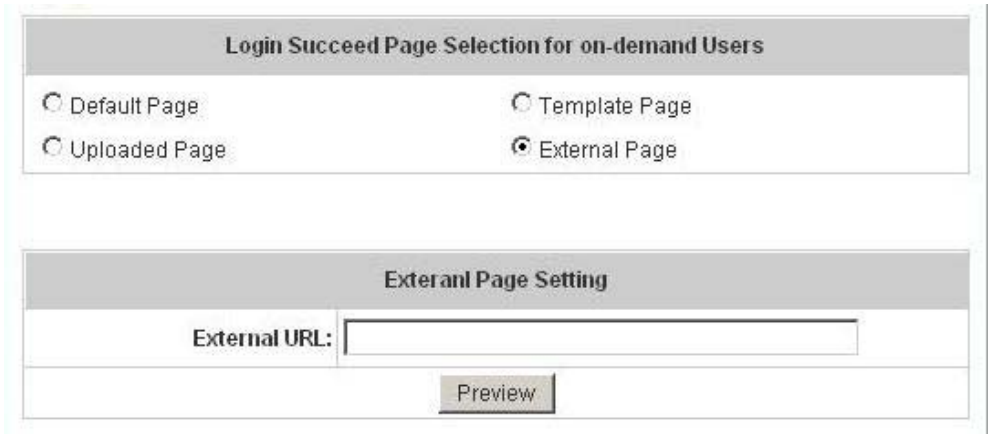
If the user-defined login succeed page for On-Demand includes an image file, the image file path in the HTML code must be the image file to be uploaded.

```
<img src="images/xx.jpg">
```

Enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login succeed page for On-Demand, click the ***Use Default Page*** button to restore it to default.

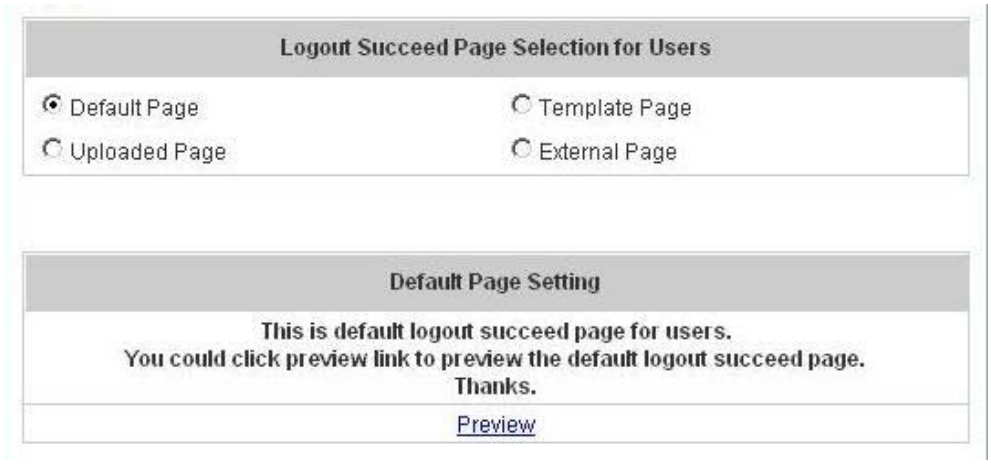
After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.

d. Choose the ***External Page*** selection and get the login succeed page for On-Demand from the specific website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***. After applying the setting, the new login succeed page for On-Demand can be previewed by clicking ***Preview*** button at the bottom of this page.

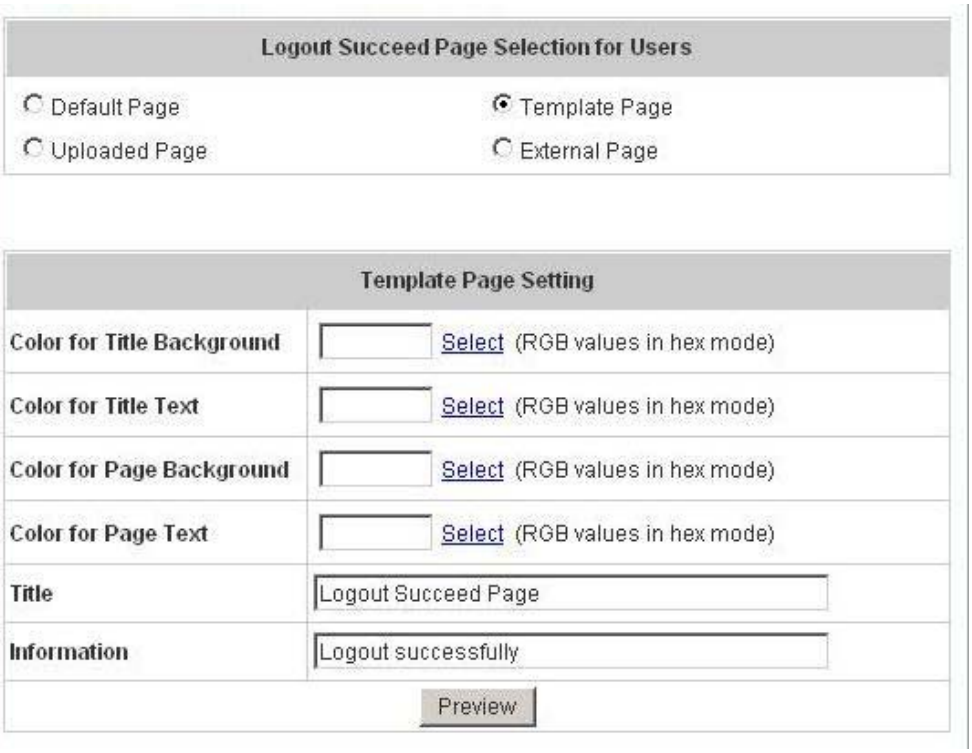


6. **Logout Succeed Page:** The administrator can use the default logout succeed page or get the customized login succeed page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click ***Preview*** to see the logout succeed page.

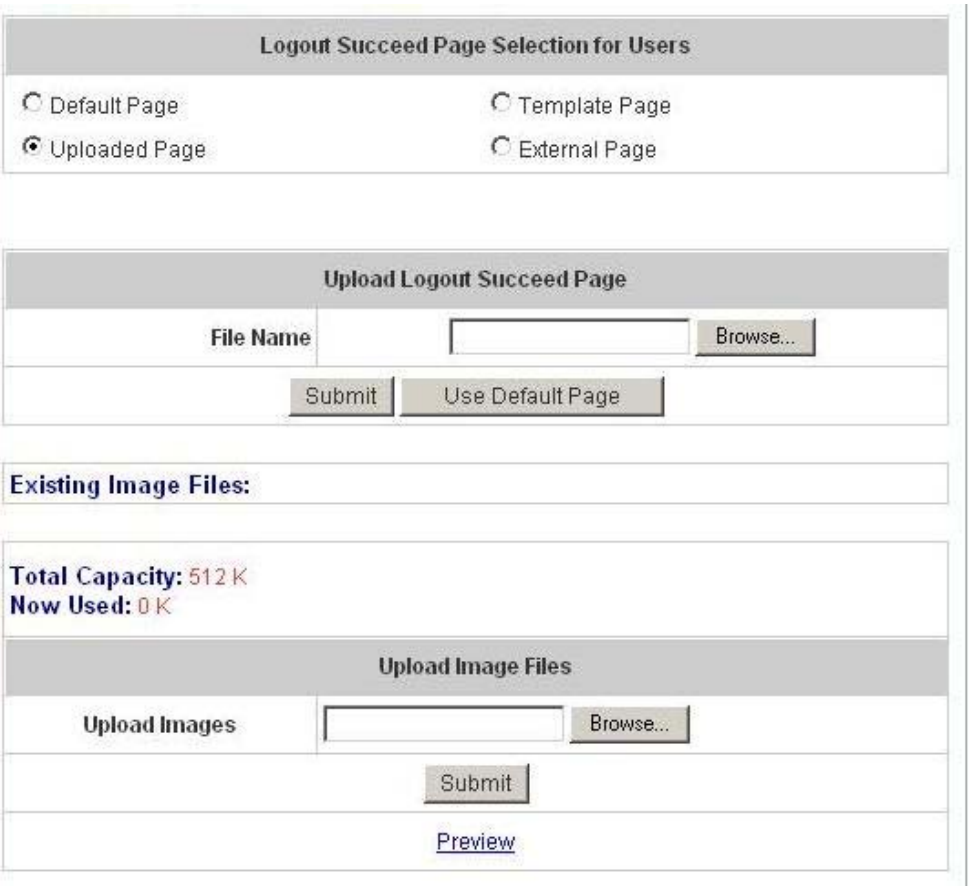
a. Choose ***Default Page*** to use the default logout succeed page.



b. Choose ***Template Page*** to make a customized logout succeed page here. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



c. Choose ***Uploaded Page*** and click the ***Browse*** button to select the file for the logout succeed page upload. Then click ***Submit*** to complete the upload process.



After the upload process is completed, the new logout succeed page can be previewed by clicking ***Preview***

button at the bottom.

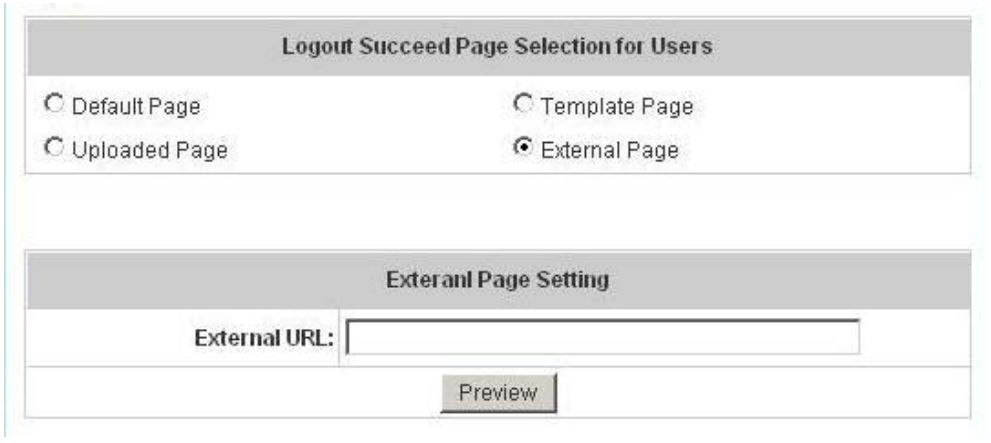
If the user-defined logout succeed page includes an image file, the image file path in the HTML code must be the image file to be uploaded.

```
<img src="images/xx.jpg">
```

Enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login succeed page, click the ***Use Default Page*** button to restore it to default.

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.

d. Choose the ***External Page*** selection and get the logout succeed page from the specific website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***. After applying the setting, the new logout succeed page can be previewed by clicking ***Preview*** button at the bottom of this page.

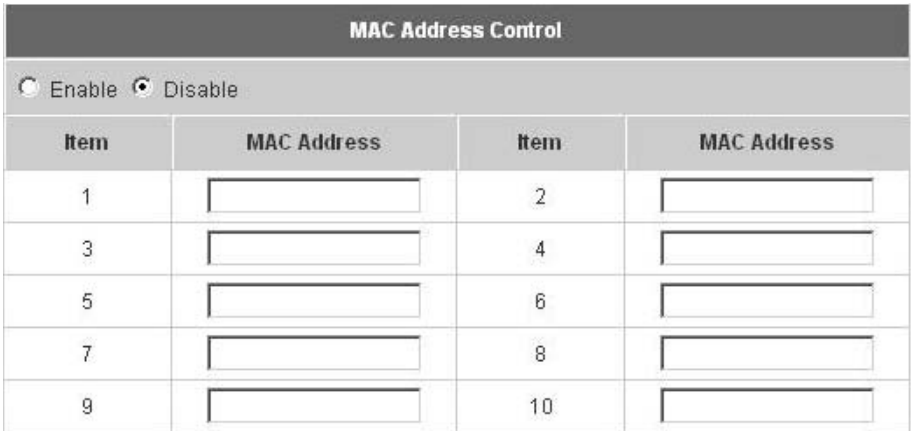


- **Credit Reminder:** The administrator can enable this function to remind the on-demand users before their credit

run out. There are two kinds of reminder, **Volume** and **Time**. The default reminding trigger level for **Volume** is 1Mbyte and the level for **Time** is 5 minutes.

- **POP3 Message:** Before the users log into the network with their usernames and passwords, the users will receive a welcome mail from WAS-102R. The administrator can edit the contents.

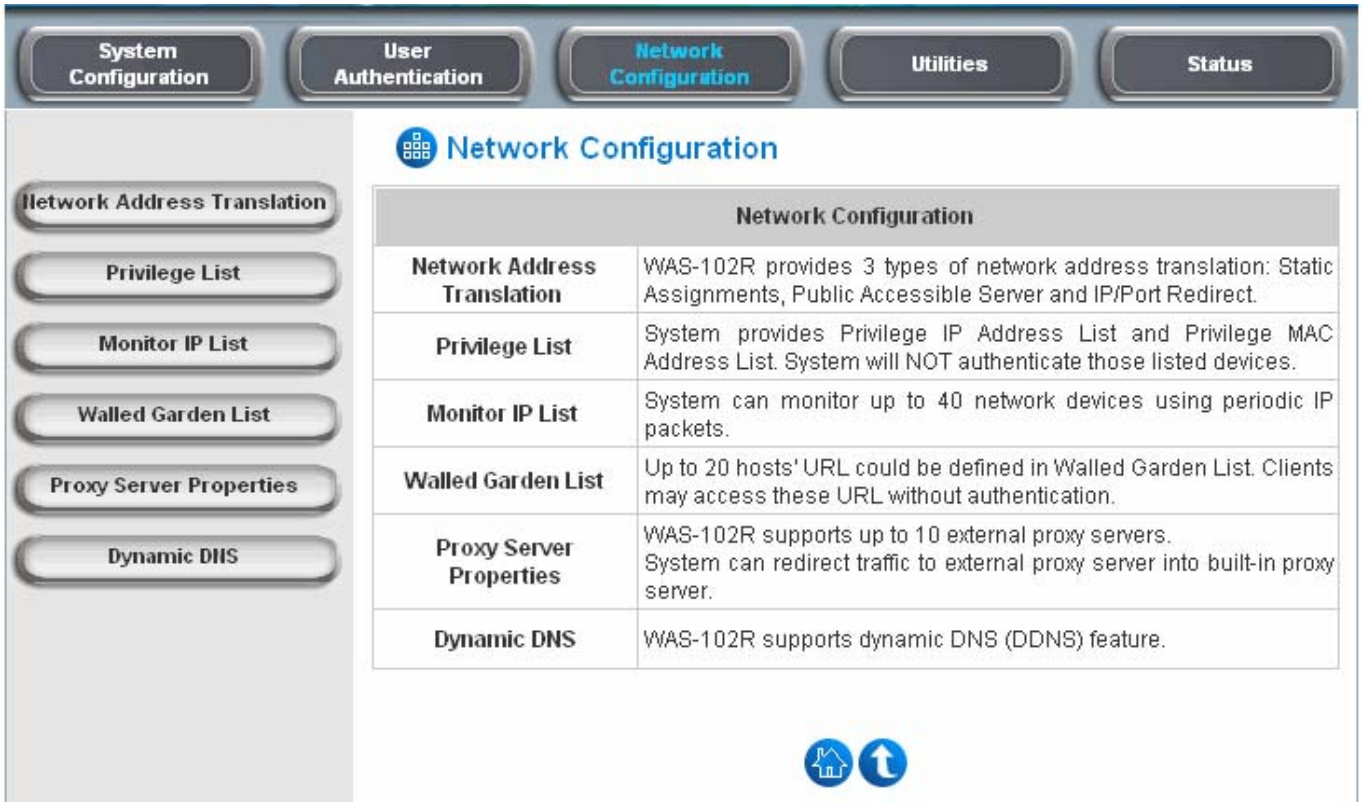
- **Enhance User Authentication:** With this function, only the users with their MAC addresses in this list can log into WAS-102R. However, user authentication is still required for these users. Please enter the **Permit MAC Address List** to fill in these MAC addresses, select **Enable**, and then click ***Apply***.



Caution: *The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.*

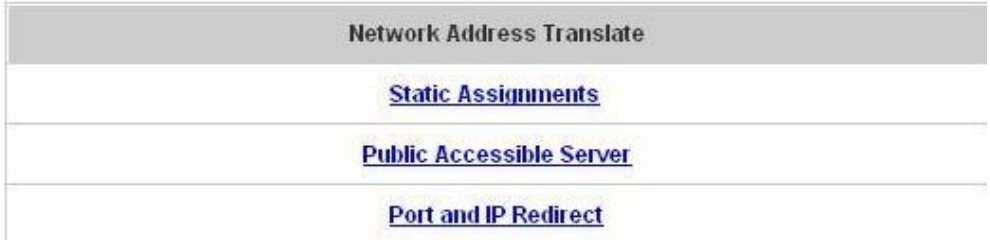
4.3 Network Configuration

This section includes the following functions: **Network Address Translation**, **Privilege List**, **Monitor IP List**, **Walled Garden List**, **Proxy Server Properties** and **Dynamic DNS**.


System Configuration
User Authentication
Network Configuration
Utilities
Status
Network Address Translation
Privilege List
Monitor IP List
Walled Garden List
Proxy Server Properties
Dynamic DNS
Network Configuration
Network Configuration
Network Address Translation
WAS-102R provides 3 types of network address translation: Static Assignments, Public Accessible Server and IP/Port Redirect.
Privilege List
System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices.
Monitor IP List
System can monitor up to 40 network devices using periodic IP packets.
Walled Garden List
Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
Proxy Server Properties
WAS-102R supports up to 10 external proxy servers.
System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS
WAS-102R supports dynamic DNS (DDNS) feature.

4.3.1 Network Address Translation

There are three parts, **Static Assignment, Public Accessible Server** and **Port and Redirect**, need to be set.



- **Static Assignment**

  A computer within the Static Assignment is unprotected by firewall and typically all port accesses are routed through to that computer. A router will forward all traffic to the computer specified in the Static Assignment if it does not otherwise have a rule for how to forward traffic on a given port. There are 40 sets of static **Internal IP Address** and **External IP Address** available. These static IP addresses can be set to the any host which itself needs a static IP address to access the network through WAN port. These settings will become effective immediately after clicking the ***Apply*** button.

Static Assignments		
Item	Internal IP Address	External IP Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(Total:40) First Prev Next Last

- **Public Accessible Server**

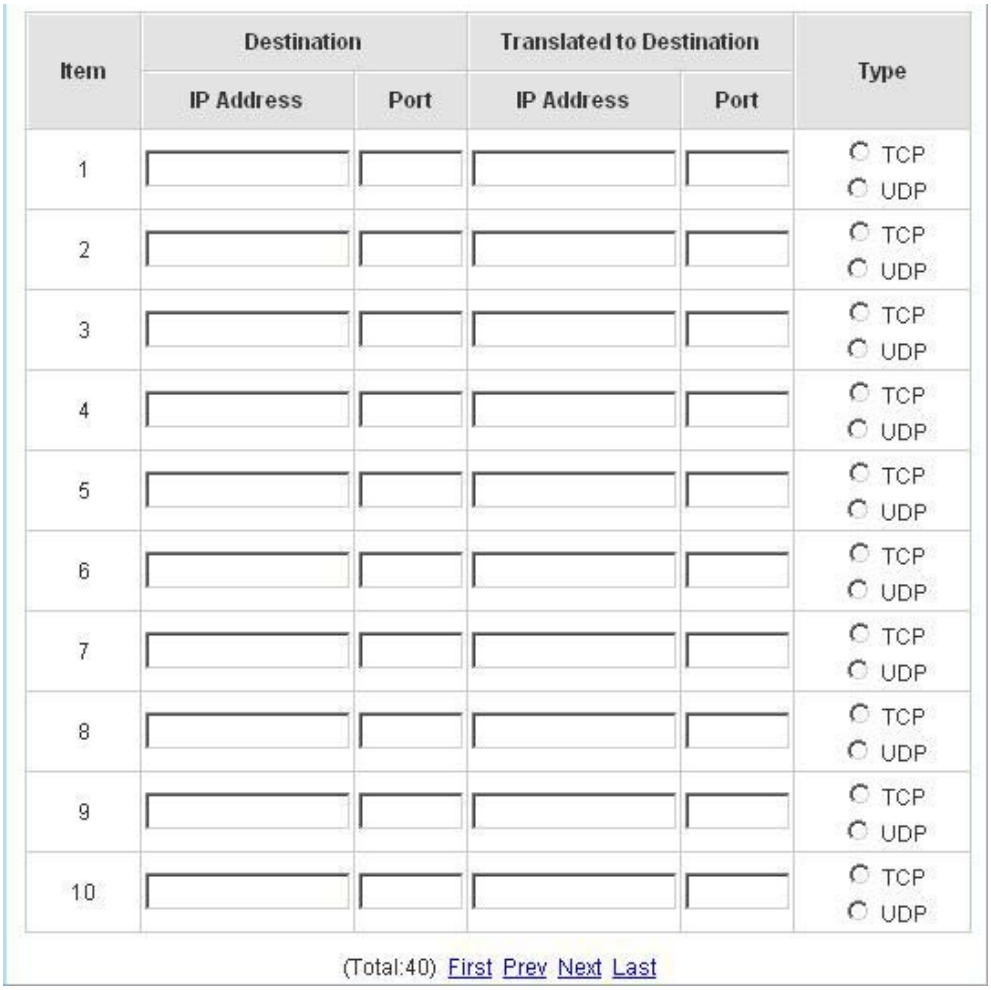
  This function allows the administrator to set 40 virtual servers at most, so that the computers not belonging to the managed network can access the servers in the managed network. Please enter the **"External Service Port"**, **"Local Server IP Address"** and **"Local Server Port"**. According to the different services provided, the network service can use the **TCP** protocol or the **UDP** protocol. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the ***Apply*** button.

Public Accessible Server					
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				TCP UDP	
2				TCP UDP	
3				TCP UDP	
4				TCP UDP	
5				TCP UDP	
6				TCP UDP	
7				TCP UDP	
8				TCP UDP	
9				TCP UDP	
10				TCP UDP	

(Total:40) First Prev Next Last

- **Port and IP Redirect**

  This function allows the administrator to set 40 sets of the IP addresses at most for redirection purpose. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the **"IP Address"** and **"Port"** of **Destination**, and the **"IP Address"** and **"Port"** of **Translated to Destination**. According to the different services provided, choose the **"TCP"** protocol or the **"UDP"** protocol. These settings will become effective immediately after clicking ***Apply***.



Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1					TCP UDP
2					TCP UDP
3					TCP UDP
4					TCP UDP
5					TCP UDP
6					TCP UDP
7					TCP UDP
8					TCP UDP
9					TCP UDP
10					TCP UDP

(Total:40) First Prev Next Last

4.3.2 Privilege List

There are two parts, **Privilege IP Address List** and **Privilege MAC Address List**, can be set.

Privilege List
Privilege IP Address List
Privilege MAC Address List

- **Privilege IP Address List**

  If there are some workstations belonging to the managed server that need to access the network without authentication, enter the IP addresses of these workstations in this list. The **"Remark"** blank is not necessary but is useful to keep track. WAS-102R allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking ***Apply***.

Pivilege IP Address List		
Item	Privilege IP Address	Remark
1		
2		
3		
4		
5		

Warning: *Permitting specific IP addresses to have network access rights without going through standard authentication process at the Public LAN (LAN1/LAN2) may cause security problems.*

- **Privilege MAC Address List**

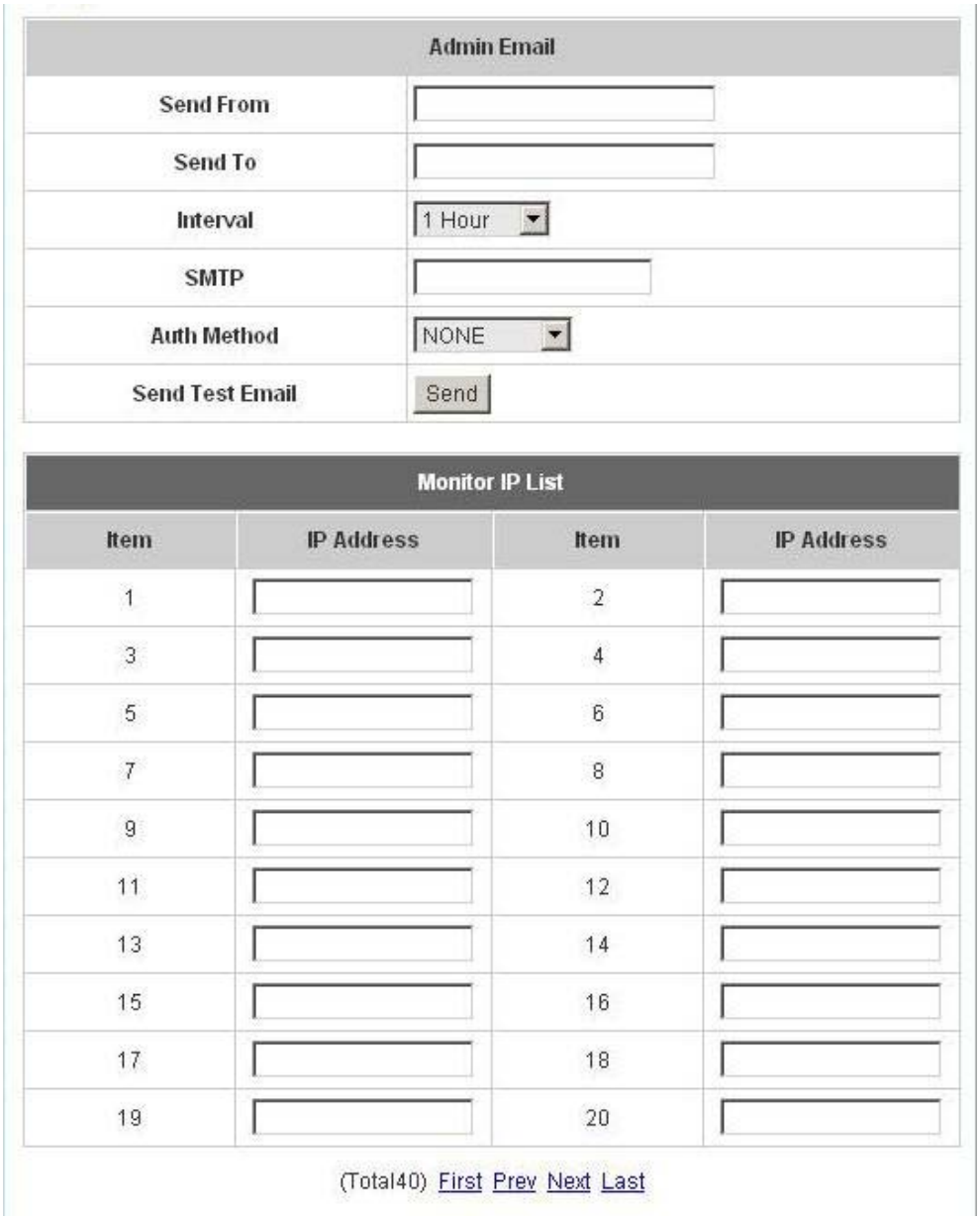
  In addition to the IP address, the MAC address of the workstations that need to access the network without authentication can also be set in this list. WAS-102R allows 100 privilege MAC addresses at most.
  When manually creating the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (not necessary). These settings will become effective immediately after clicking ***Apply***.

Privilege MAC Address List		
Item	MAC Address	Remark
1		
2		
3		
4		
5		

Warning: *Permitting specific MAC addresses to have network access rights without going through standard authentication process at the Public LAN (LAN1/LAN2) may cause security problems.*

4.3.3 Monitor IP List

WAS-102R will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the related information, click ***Apply*** and these settings will become effective immediately. Click ***Monitor*** to check the current status of all the monitored IP. The system provides 40 IP addresses for the **"Monitor IP List"**.



- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person whom the monitoring result is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Server:** The IP address of the SMTP server.

- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method selected, enter the **Account Name**, **Password** and **Domain**.
- **Send Test Email:** To test the settings correct or not.
- **Monitor IP Address:** The IP addresses under monitoring.

Monitor IP result		
No	IP Address	Result
1	192.168.1.200	
2	192.168.1.100	

4.3.4 Walled Garden List

This function provides some free services to the users to access websites listed here before login and authentication. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Please enter the website **IP Address** or **Domain Name** in the list and these settings will become effective immediately after clicking ***Apply***.

Walled Garden List			
Item	Addres	Item	Addres
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

4.3.5 Proxy Server Properties

WAS-102R supports Internal Proxy Server and External Proxy Server functions. Please select an **Access Gateway** and then perform the necessary configurations.

External Proxy Server

Item	Server IP	Port
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

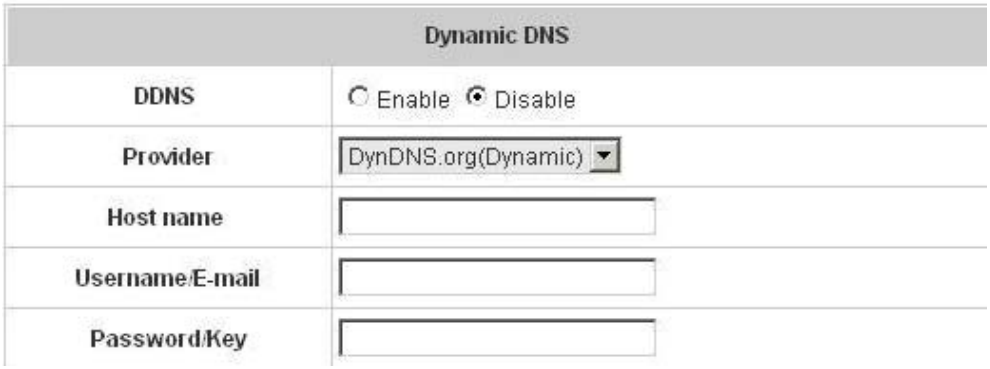
Internal Proxy Server

Built-in Proxy Server	○ Enable ◉ Disable

- **External Proxy Server:** Under the WAS-102R security management, the system will match the External Proxy Server list to the end-users' proxy setting. If there isn't a match, then the end-users will no be able to reach the login page and thus unable to access the network. If there is a match, the end-users will be directed to the system first for authentication. After a successful authentication, the end-users will be redirected back to the desired proxy servers depending on various situations.
- **Internal Proxy Server:** WAS-102R has a built-in proxy server. If this function is enabled, the end users will be forced to treat WAS-102R as the proxy server regardless of the end-users' original proxy settings.
  For more details about how to set up the proxy servers, please refer to Appendix C and Appendix D.

4.3.6 Dynamic DNS

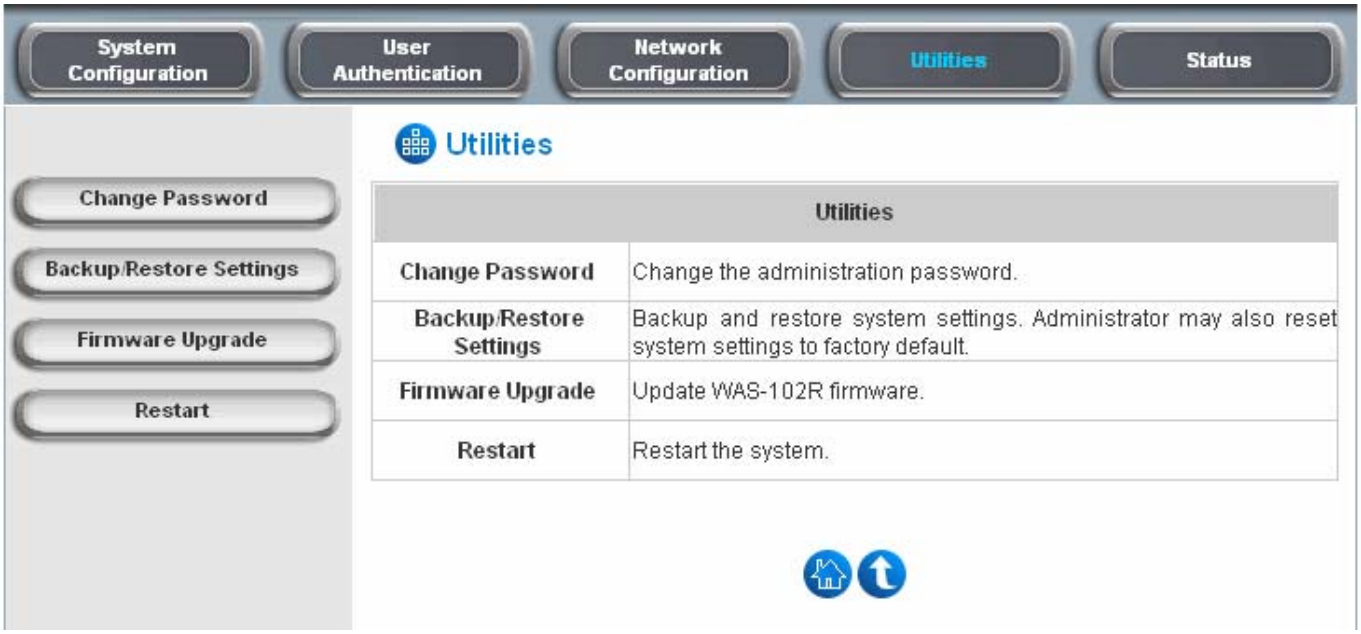
WAS-102R provides a convenient DNS function to translate the IP address of WAN port to a domain name that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server. These settings will become effective immediately after clicking ***Apply***.



- **DDNS:** Enabling or disabling of this function.
- **Provider:** Select the DNS provider.
- **Host name:** The IP address/domain name of the WAN port.
- **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- **Password/Key:** The register password for the DNS provider.

4.4 Utilities

This section provides four utilities to customize and maintain the system including **Change Password**, **Backup/Restore Setting**, **Firmware Upgrade** and **Restart**.



4.4.1 Change Password

There are three levels of authorities to use: **admin**, **manager** or **operator**. The default usernames and passwords are as follow:

Admin: The administrator can access all configuration pages of the WAS-102R.

User Name: **admin**

Password: **admin**

Manager: The manager can only access the configuration pages under ***User Authentication*** to manage the user accounts, but has no permission to change the settings of the profiles for Firewall, Specific Route and Schedule.

User Name: **manager**

Password: **manager**

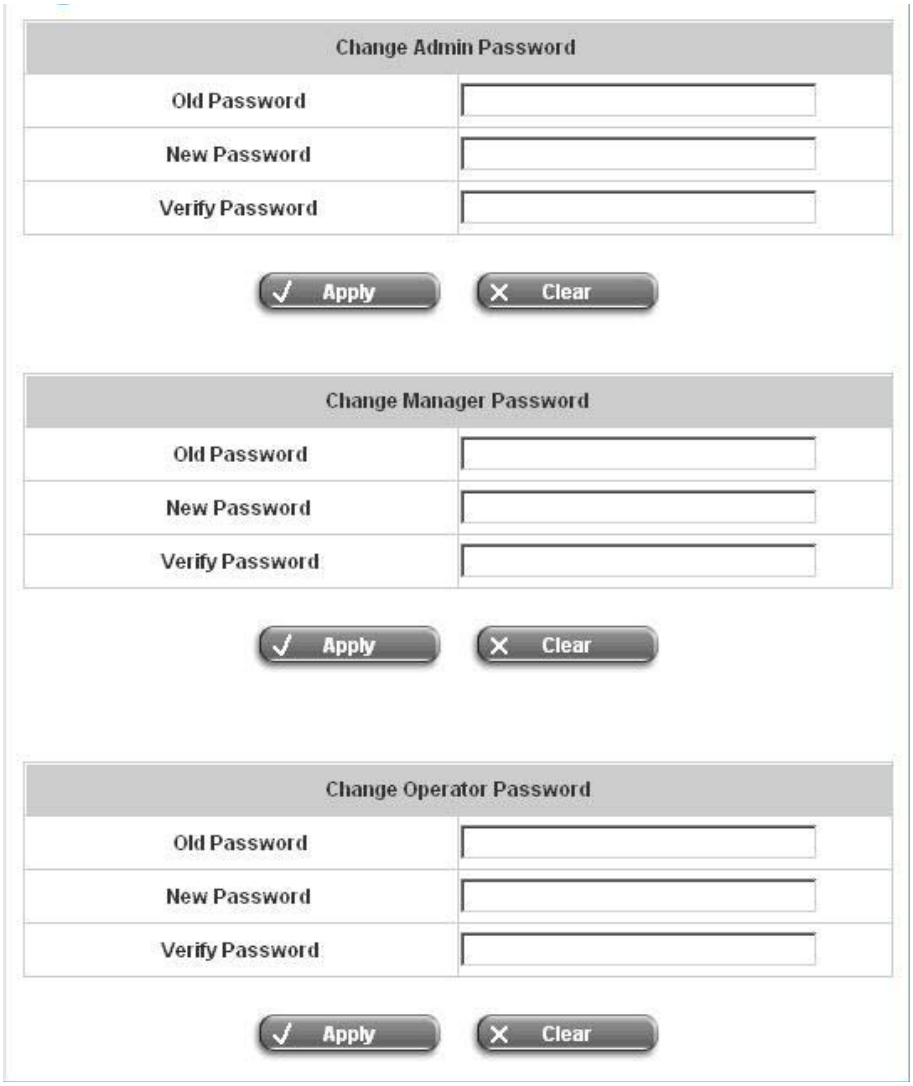
Operator: The operator can only access the configuration page of ***Create On-demand User*** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **operator**

The administrator can change the passwords here. Please enter the current password and then enter the new

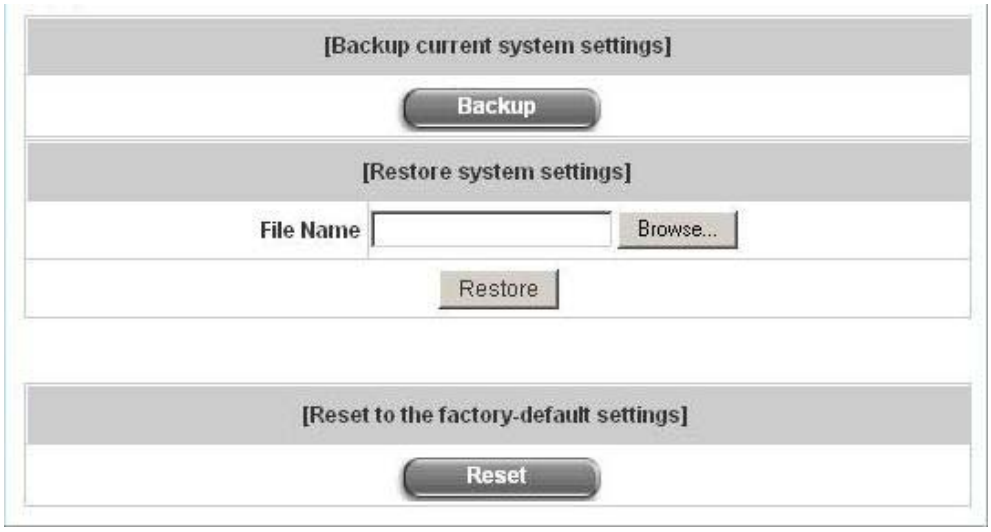
password twice to verify. Click ***Apply*** to activate this new password.



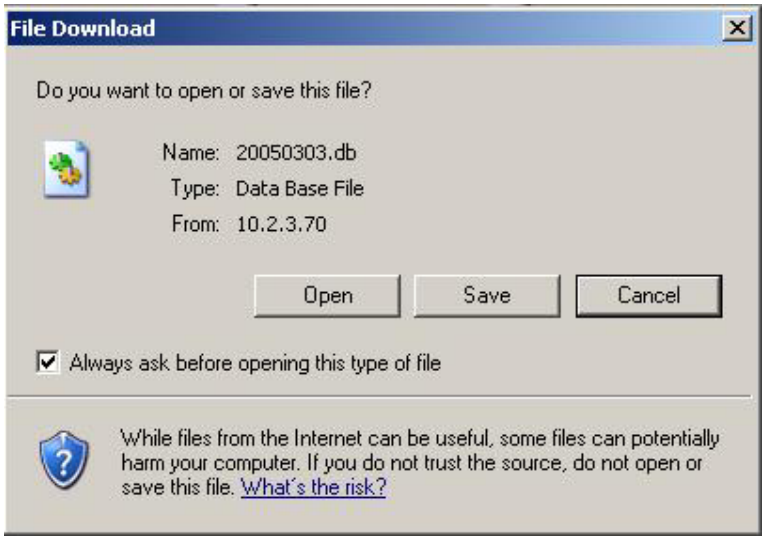
Caution: *If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port, console/printer port.*

4.4.2 Backup/Restore Setting

This function is used to backup/restore the WAS-102R settings. Also, WAS-102R can be restored to the factory default settings here.



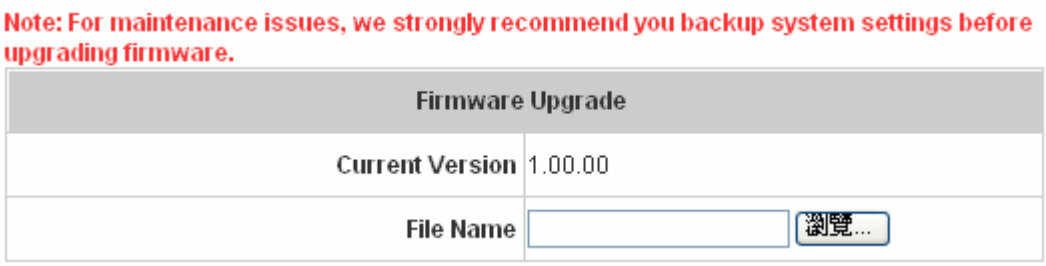
- **Backup Current System Setting:** Click ***Backup*** to create a .db database backup file and save it on disk.


File Download
Do you want to open or save this file?
Name: 20050303.db
Type: Data Base File
From: 10.2.3.70
Open
Save
Cancel
Always ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

- **Restore System Setting:** Click ***Browse*** to search for a .db database backup file created by WAS-102R and click ***Restore*** to restore to the same settings at the time the backup file was created.
- **Resetting to the Factory-Default configuration:** Click ***Reset*** to load the factory default settings of WAS-102R.

4.4.3 Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click ***Browse*** to search for the firmware file and click ***Apply*** to go on with the firmware upgrade process. It might be a few minutes before the upgrade process completes and the system needs to be restarted afterwards to make the new firmware effective.



Warning: *1. Firmware upgrade may cause the loss of some of the data. Please refer to the release notes for the limitation before upgrading the firmware. 2. Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or the restart process. It may damage the system and cause it to malfunction.*

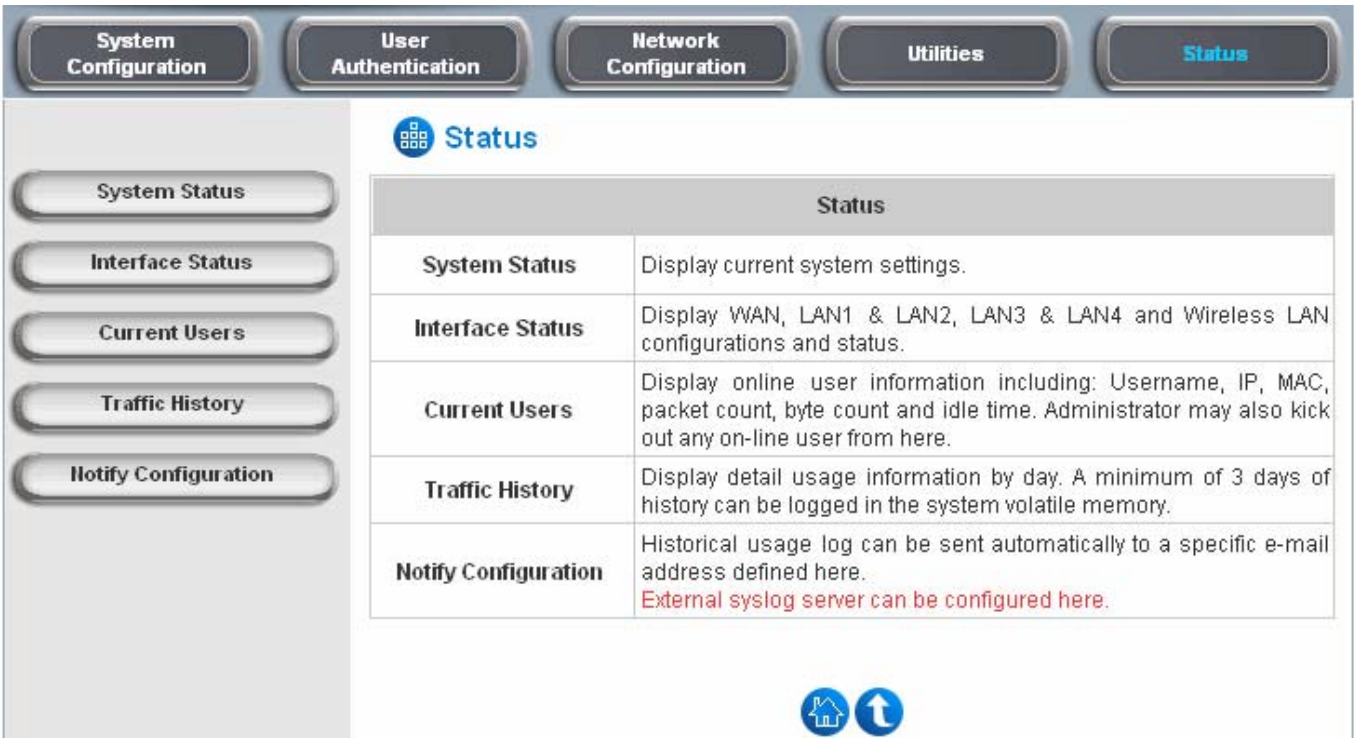
4.4.4 Restart

This function allows the administrator to safely restart WAS-102R and the process should take about three minutes. Click ***YES*** to restart WAS-102R; click ***NO*** to go back to the previous screen. If the power needs to be turned off, restarting WAS-102R first and then turning off the power after completing the restart process is highly recommended.

Caution: *The connection of all online users of the system will be disconnected when system is in the process of restarting.*

4.5 Status

This section includes **System Status**, **Interface Status**, **Current Users**, **Traffic History**, and **Notification Configuration** to provide system status information and online user status.


System Configuration
User Authentication
Network Configuration
Utilities
Status
System Status
Interface Status
Current Users
Traffic History
Notify Configuration
Status
Status
System Status
Display current system settings.
Interface Status
Display WAN, LAN1 & LAN2, LAN3 & LAN4 and Wireless LAN configurations and status.
Current Users
Display online user information including: Username, IP, MAC, packet count, byte count and idle time. Administrator may also kick out any on-line user from here.
Traffic History
Display detail usage information by day. A minimum of 3 days of history can be logged in the system volatile memory.
Notify Configuration
Historical usage log can be sent automatically to a specific e-mail address defined here.
External syslog server can be configured here.

4.5.1 System Status

This section provides an overview of the system for the administrator.

System Status		
Current Firmware Version		1.00.00
System Name		WAS-102R
Admin info		Sorry! The service is temporarily unavailable.
Home Page		http://www.pheenet.com
Syslog server-Traffic History		N/A:N/A
Syslog server-On demand User log		N/A:N/A
Proxy Server		Disabled
Friendly Logout		Enabled
Internet Connection Detection		Disabled
Management	Remote Management IP	0.0.0.0/0.0.0.0
	SNMP	Disabled
History	Retained Days	3 days
	Traffic log Email To	N/A
	On-demand log Email To	N/A
Time	NTP Server	(tock.usno.navy.mil)
	Date Time	2006/07/02 04:37:02 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
	Guest Account	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A

The description of the table is as follows:

Item	***Description***
Current Firmware Version	The present firmware version of WAS-102R
System Name	The system name. The default is WAS-102R
Admin Info	The information to be shown on the login screen when a user has a connection problem.
Home Page	The page to which the users are directed after successful login.
Syslog server-Traffic History	The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.

Syslog server-On demand User log		The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Proxy Server		Enabled/disabled stands for that the system is currently using the proxy server or not.
Friendly Logout		Enabled/disabled stands for the setting of hiding/displaying an extra confirmation window when users click the logout button.
Internet Connection Detection		Enabled/Disabled stands for the connection at WAN is normal or abnormal (**Internet Connection Detection**) and all online users are allowed/disallowed to log in the network.
Management	**Remote Management IP**	The IP or IPs that is allowed for accessing the management interface.
	SNMP	Enabled/disabled stands for the current status of the SNMP management function.
History	**Retained Days**	The maximum number of days for the system to retain the users' information.
	Traffic log Email To	The email address to which that the traffic history information will be sent.
	On-demand log Email To	The email address to which the history information about on-demand users is sent.
Time	**NTP Server**	The network time server that the system is set to align.
	Date Time(GMT+0:00)	The system time is shown as the local time.
User	**Idle Timer**	The minutes allowed for the users to be inactive.
	Multiple Login	Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account.
	Guest Account	Enabled/disabled stands for the current status of allowing Guest Accounts to log in.
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

4.5.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN**, **LAN1 & LAN2**, **LAN3 & LAN4,** and **Wireless Port**.

Interface Status		
WAN	MAC Address	00:11:A3:03:AF:39
	IP Address	169.254.175.57
	Subnet Mask	255.255.255.255
Wireless	Operation Mode	NAT
	MAC Address	00:14:85:CE:7D:85
	IP Address	192.168.3.254
	Subnet Mask	255.255.255.0
	SSID	default
	Channel	1
	Encryption Function	Disabled
Wireless DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.3.100
	End IP Address	192.168.3.200
	Lease Time	1440 Min(s)
LAN1 & LAN2	Mode	NAT
	MAC Address	00:11:A3:03:AF:38
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
LAN1 & LAN2 DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.1
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
LAN3 & LAN4	Mode	NAT
	MAC Address	00:11:A3:03:AF:38
	IP Address	192.168.2.254

	Subnet Mask	255.255.255.0
LAN3 & LAN4 DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.2.1
	End IP Address	192.168.2.100
	Lease Time	1440 Min(s)

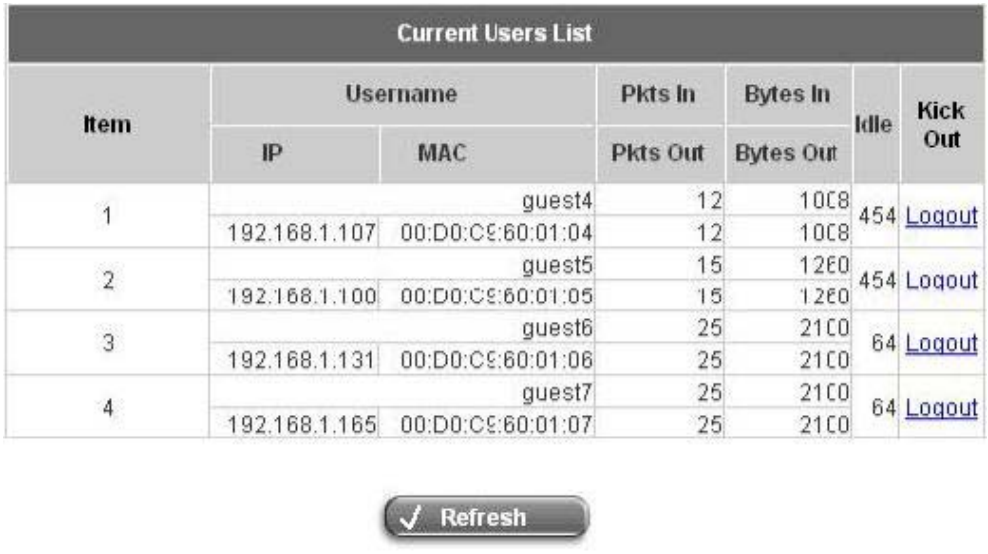
The description of the table is as follows.

Item		***Description***
WAN	**MAC Address**	The MAC address of the WAN port.
	IP Address	The IP address of the WAN port.
	Subnet Mask	The Subnet Mask of the WAN port.
Wireless	**Operation Mode**	The mode of the wireless port.
	MAC Address	The MAC address of the wireless port.
	IP Address	The IP address of the wireless port.
	Subnet Mask	The Subnet Mask of the wireless port.
	SSID	The ESSID of the wireless port.
	Channel	The assigned Channel of the Wireless port.
	Encryption Function	Enabled/disabled stands for the status of the encryption function of the wireless port.
Wireless DHCP Server	**Status**	Enable/disable stands for status of the DHCP server on the Wireless port.
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.
LAN1 & LAN2	**Mode**	The mode of the LAN1 & LAN2 port.
	MAC Address	The MAC address of the LAN1 & LAN2.
	IP Address	The IP address of the LAN1 & LAN2.
	Subnet Mask	The Subnet Mask of the LAN1 & LAN2.
LAN1 & LAN2 DHCP Server	**Status**	Enable/disable stands for status of the DHCP server on the LAN1 & LAN2.
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.

	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.
LAN3 & LAN4	**Mode**	The mode of the LAN3 & LAN4.
	MAC Address	The MAC address of the LAN3 & LAN4.
	IP Address	The IP address of the LAN3 & LAN4.
	Subnet Mask	The Subnet Mask of the LAN3 & LAN4.
LAN3 & LAN4 DHCP Server	**Status**	Enable/disable stands for status of the DHCP server on the LAN3 & LAN4 port
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP Address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.

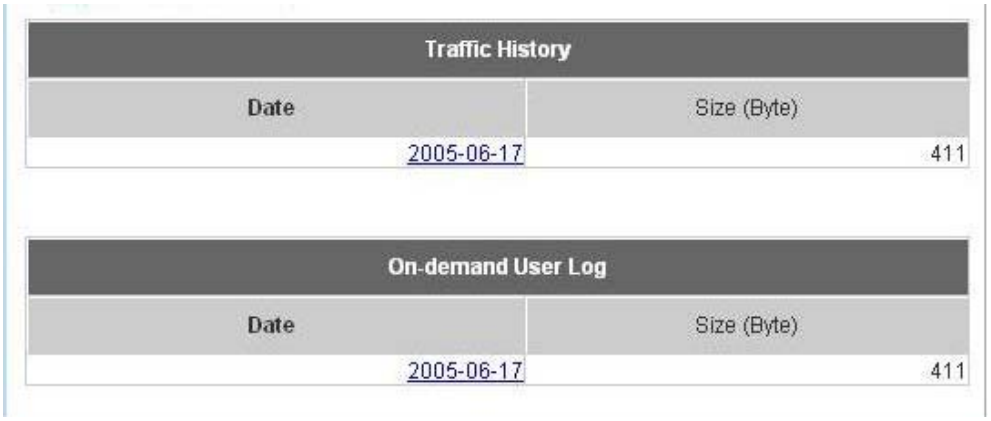
4.5.3 Current Users

In this function, each online user's information including **Username**, **IP Address**, **MAC Address**, **Packets In**, **Bytes In**, **Packets Out**, **Bytes Out, Idle Time** and **Logout** can be obtained. Administrator can use this function to force a specific online user to log out. Click the hyperlink of ***Logout*** next to the online user's name to logout that particular user. Click ***Refresh*** to renew the current users list.



4.5.4 Traffic History

This function is used to check the history of WAS-102R. The history of each day will be saved separately in the DRAM for at least3 days.



Traffic History	
Date	Size (Byte)
2005-06-17	411

On-demand User Log	
Date	Size (Byte)
2005-06-17	411

Caution: *Since the history is saved in the DRAM, if you need to restart the system and also keep the history, then please manually copy and save the information before restarting.*

If the **History Email** has been entered under the **Notify Configuration** page, then the system will automatically send out the history information to that email address.

- **Traffic History**

  As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type, Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out,** and **Bytes Out**, of user activities.

Traffic History 2005-03-22								
Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out
2005-03-22 19:12:21 +0800	LOGIN	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0
2005-03-22 19:12:24 +0800	LOGOUT	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252
2005-03-22 19:12:29 +0800	LOGIN	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0
2005-03-22 19:12:32 +0800	LOGOUT	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252
2005-03-22 19:13:51 +0800	LOGIN	user1@local.tw	192.168.1.1	00:D0:C9:60:01:01	0	0	0	0

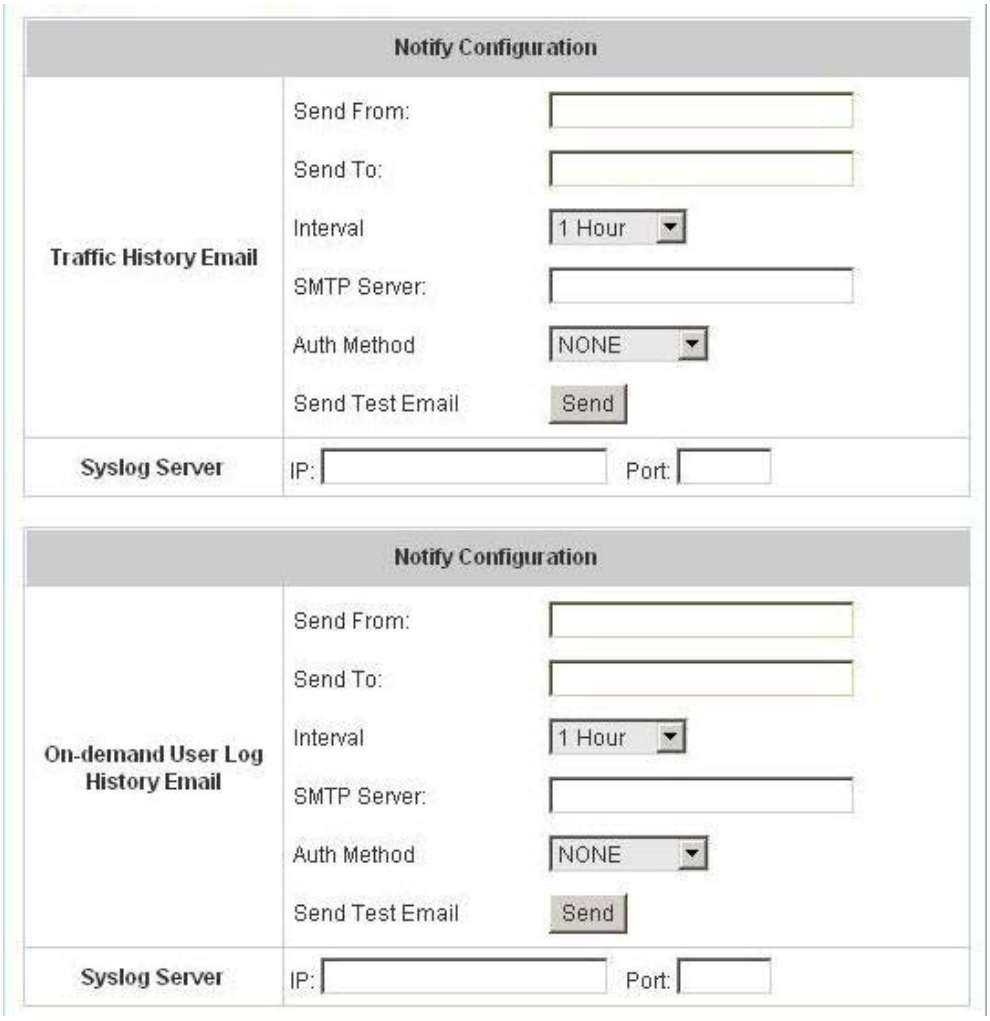
- **On-demand User Log**

  As shown in the following figure, each line is a on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, Expiretime**, **Validation** and **Remark**, of user activities.

On-demand User Log 2005-03-22												
Date	System Name	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	Expiretime	Validtime	Remark
2005-03-22 17:55:58 +0800	My Service	Create_OD_User	P4SP	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:55:58	None	2 hrs 0 mins
2005-03-22 17:56:03 +0800	My Service	Create_OD_User	62H6	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:56:03	None	2 hrs 0 mins
2005-03-22 17:56:07 +0800	My Service	Create_OD_User	886D	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:56:07	None	2 hrs 0 mins

4.5.5 Notify Configuration

The WAS-102R will save the traffic history into the internal DRAM. If the administrator wants the system to automatically send out the history to a particular email address, please enter the related information in these fields.



- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person whom the history email is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Server:** The IP address of the SMTP server.
- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method selected, enter the **Account Name**, **Password** and **Domain**.

  NTLMv1 is not currently available for general use.

  Plain and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**. Outlook and Outlook express use **Login** as default, although they can be set to use **NTLMv1**.

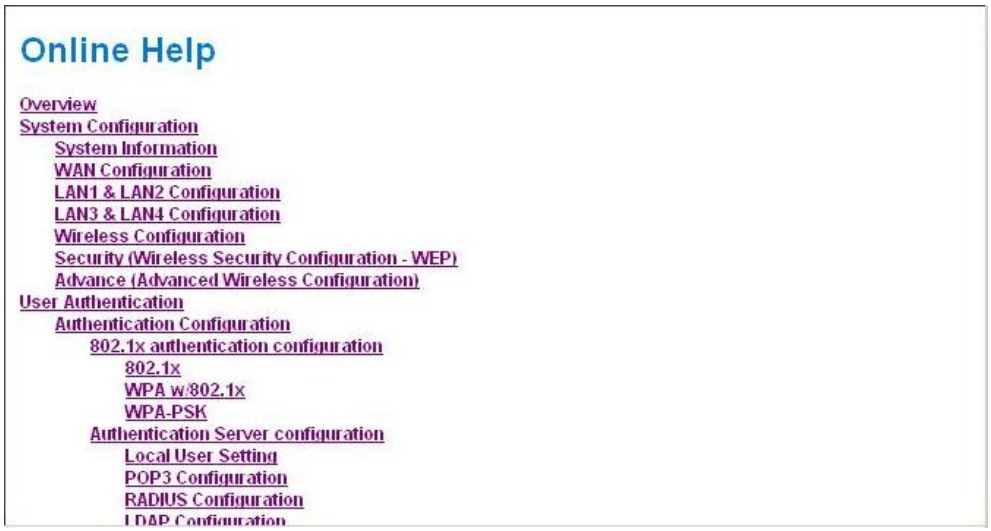
  Pegasus uses **CRAM-MD5** or **Login** but administrators can not configure which method to be used.

- **Send Test Email:** To test the settings correct or not.
- **Syslog Server:** It specifies the IP and Port of the Syslog server.

4.6 Help

On the screen, the **Help** button is on the upper right corner.

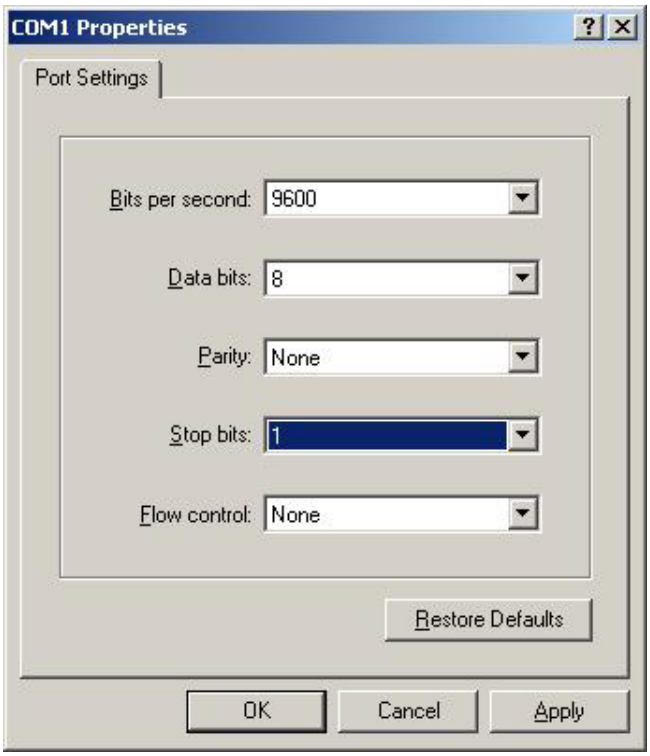
Click ***Help*** to the **Online Help** window and then click the hyperlink of the items to get the information.



5. Appendix A -- Console Interface

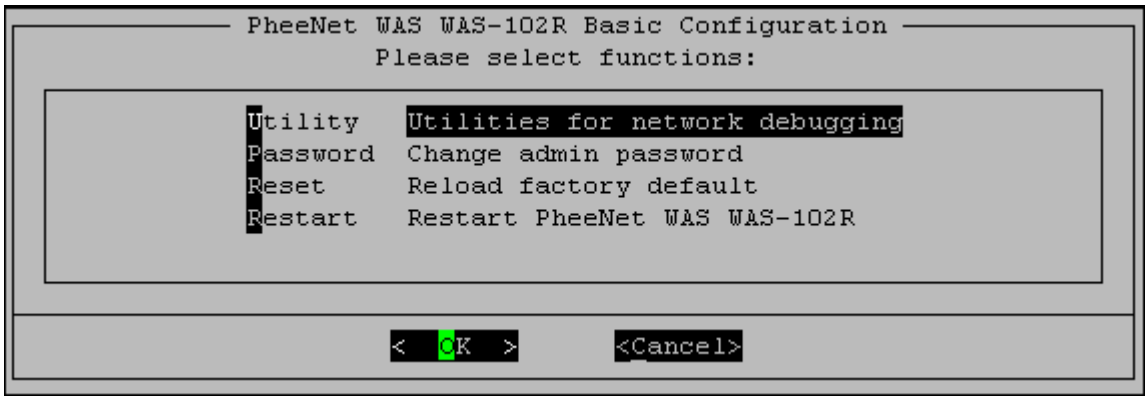
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. In order to connect to the console port of WAS-102R, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **9600,8,n,1**.



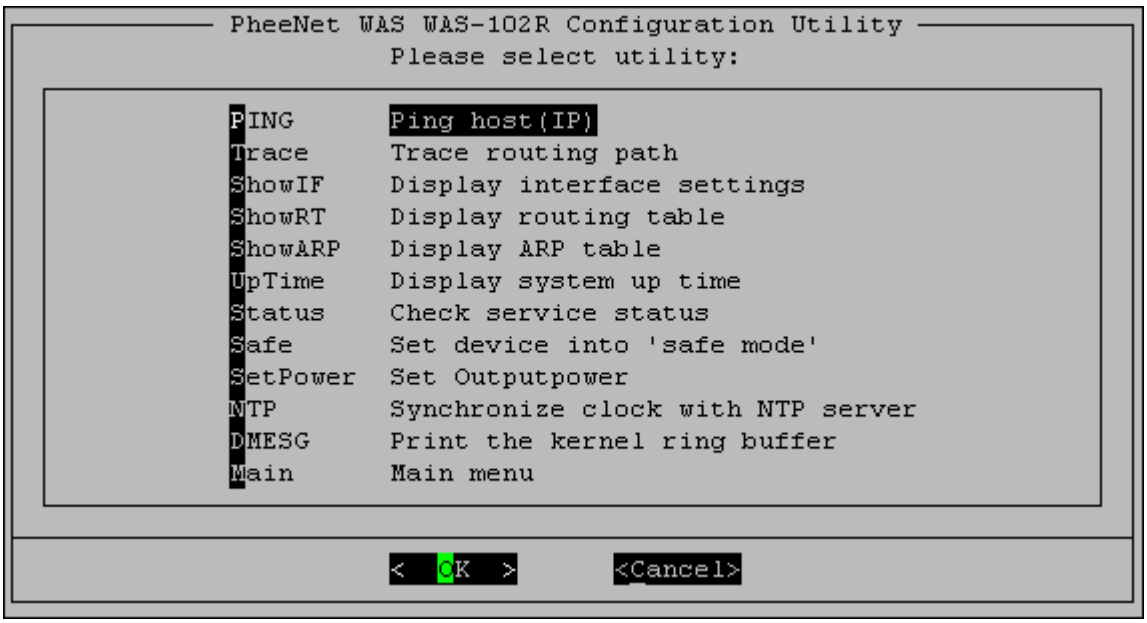
Caution: *the main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the* ***Enter*** *key to make selection or confirm what you enter.*

3. Once the console port of WAS-102R is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system and the welcome screen or the main menu should appear. If the welcome screen or the main menu of the console still can not show up, please check the connection of the cables and the settings of the terminal simulation program.


PheeNet WAS WAS-102R Basic Configuration
Please select functions:
Utility Utilities for network debugging
Password Change admin password
Reset Reload factory default
Restart Restart PheeNet WAS WAS-102R
< OK >
<Cancel>

- **Utilities for network debugging**

  The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follow:


PheeNet WAS WAS-102R Configuration Utility
Please select utility:
PING Ping host(IP)
Trace Trace routing path
ShowIF Display interface settings
ShowRT Display routing table
ShowARP Display ARP table
UpTime Display system up time
Status Check service status
Safe Set device into 'safe mode'
SetPower Set Outputpower
NTP Synchronize clock with NTP server
DMESG Print the kernel ring buffer
Main Main menu
< OK >
<Cancel>

  - Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
  - Trace routing path: Trace and inquire the routing path to a specific target.
  - Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
  - Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
  - Display ARP table: The internal ARP table of the system is displayed.
  - Display system up time: The system live time (time for system being turn on) is displayed.
  - Check service status: Check and display the status of the system.
  - Set device into "safe mode": If administrator is unable to use Web Management Interface via the browser for the system failed inexplicitly. Administrator can choose this utility and set AMG-2000 into safe mode, then administrator can management this device with browser again.
  - Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.
  - Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their bootup messages instead of copying the messages by hand.
  - Main menu: Go back to the main menu.

- **Change admin password**

  Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to

the system console, we do not need to enter administrator's password to enter the console management interface. But connecting the system by SSH, we have to enter the username and password.

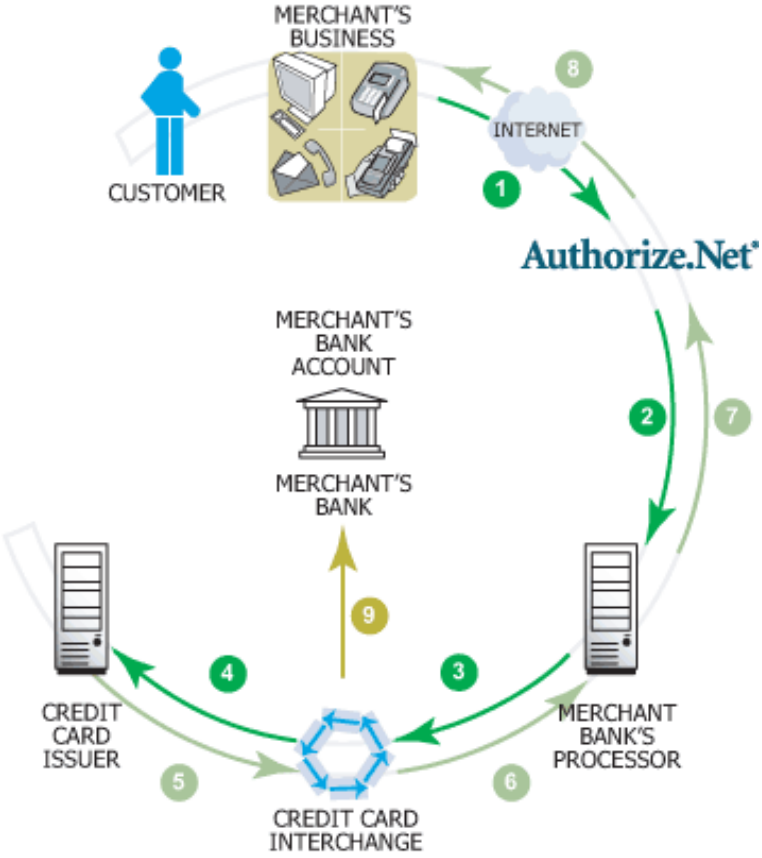
The username is "admin" and the default password is also "admin", which is the same as for the web management interface. Password can also be changed here. if administrators forget the password and are unable to log in the management interface from the web or the remote end of the SSH, they can still use the null modem to connect the console management interface and set the administrator's password again.

Caution: *Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the WAS-102R Admin username and password after logging in the system for the first time.*

- **Reload factory default**
  Choosing this option will reset the system configuration to the factory defaults.
- **Restart WAS-102R**
  Choosing this option will restart WAS-102R.

6. Appendix B -- Configuration on Authorize.Net

Before the "Credit Card" and related functions can be managed appropriately, WAS-102R requires the merchant owners to have a valid **Authorize.Net** (www.authorize.net) account, since Authorize.Net is the on-line payment gateway that WAS-102R supports now. The figure below shows the process of the credit card billing and we will introduce some important procedures for configurations on Authorize.Net.



1. Setting Up

1.1 Open Accounts

As shown in the above figure, four elements are needed to begin an on-line business:

Element	Description
E-COMMERCE WEB SITE	WAS-102R has built-in web pages to present to end users to use credit cards
INTERNET MERCHANT ACCOUNT	A type of bank account that allows a business to accept Internet credit card
PAYMENT GATEWAY ACCOUNT	An Authorize.Net account is the type of account that is supported by WAS-102R
CONNECTION METHOD	WAS-102R will take care of the communication with the Authorize.Net

Therefore, to set up WAS-102R to process credit card billing, the merchant owner will need two accounts (Internet Merchant account and Authorize.Net account). If you are looking for a merchant account or Internet payment gateway to process transactions, you can fill out the Inquiry Form on http://www.authorize.net/solutions/merchantsolutions/merchantinquiryform/. When the four elements are prepared, start configuring the settings on WAS-102R and Athorize.Net.

1.2 Configure WAS-102R using an Authorize.Net account

Please log in WAS-102R. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → Click ***Credit Card*** → ***Credit Card Configuration***

Some major fields are required:

Setting	Description
Merchant Login ID	This is the "Login ID" that comes with the Authorize.Net account.
Merchant Transaction Key	To get a new key, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → Click ***Obtain Transaction Key*** → Enter **"Secret Answer"** → Click ***Submit***.
Payment Gateway URL	https://secure.authorize.net/gateway/transact.dll (default payment gateway)
MD5 Hash	To enhance the transaction security, merchant owner can choose to enable this function and enter a value in the text box: **"MD5 Hash Value"**.

Note: For detailed description, please see P64 – Credit Card.

1.3 Configure the Authorize.Net Merchant Account to Match the Configuration of WAS-102R

Settings of the merchant account on Authorize.Net should be matched with the configuration of WAS-102R:

Setting	Description
MD5 Hash	To configure **"MD5 Hash Value"**, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → click ***MD5 Hash*** → Enter **"New Hash Value"** & **"Confirm Hash Value"** → Click ***Submit***.
Required Card Code	If the **"Card Code"** is set up as a required field, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → click ***Card Code Verification*** → Check the ***Does NOT Match (N)*** box → Click ***Submit***.
Required Address Fields	After setting up the required address fields on the **"Credit Card Payment Page Fields Configuration"** section of WAS-102R, the same requirements must be set on Authorize.Net. To do so, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → click ***Address Verification System (AVS)*** → Check the boxes accordingly → Click ***Submit***.

1.4 Test The Credit Card Payment via Authorize.Net

To test the connection between WAS-102R and Authorize.Net, please log in WAS-102R. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Credit Card*** → ***Credit Card Configuration*** → Go to "**Credit Card Payment Page Configuration**" section → Enable the **"Test Mode"** → Click ***Try Test*** and follow the instructions

2. Basic Maintenance

In order to maintain the operation, merchant owners will have to manage the accounts and transactions via Authorize.Net as well as WAS-102R.

2.1 Void A Transaction and Remove the On-demand Account Generate on WAS-102R

Sometimes, a transaction may need to be canceled as well as the related user account on WAS-102R before it has been settled with the bank.

a. To void an unsettled transaction, please log in Authorize.Net. Click ***Unsettled Transactions*** → Try to locate the specific transaction record on the **"List of Unsettled Transactions"** → Click the ***Trans ID*** number → Confirm and click ***Void***.

Note: *To find the on-demand account name, click* ***Show Itemized Order Information*** *in the* ***"Order Information"*** *section → Username can be found in the* ***"Item Description"***

b. To remove the specific account from WAS-102R, please log in WAS-102R. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Users List*** → Click ***Delete*** on the record with the account name.

2.2 Refund A Settled Transaction and Remove The On-demand Account Generated on WAS-102R

a. To refund a credit card, please log in Authorize.Net. Click ***Virtual Terminal*** → Select Payment Method → Click ***Refund a Credit Card*** → Payment/Authorization Information → Type information in at least three fields: Card Number, Expiration Date, and Amount → Confirm and click ***Submit***.
b. To remove the specific account from WAS-102R, please log in WAS-102R. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Users List*** → Click ***Delete*** on the record with the account name

2.3 Find the Username and Password for A Specific Customer

Please log in Authorize.Net. Click ***Unsettled Transactions*** → Try to locate the specific transaction record on the **"List of Unsettled Transactions"** → Click the ***Trans ID*** number → Click ***Show Itemized Order Information*** in the **"Order Information"** section → Username and Password can be found in the **"Item Description"**.

2.4 Send An Email Receipt to A Customer

If a valid email address is provided, WAS-102R will automatically send the customer an email receipt for each successful transaction via Authorize.Net. To change the information on the receipt for customer, please log in

WAS-102R. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Credit Card*** → ***Credit Card Configuration*** → ***Client's Purchasing Record*** → Type in information in the text boxes: **"E-mail Header and Description"** → Confirm and click ***Apply***.

2.5 Send An Email Receipt for Each Transaction to The Merchant Owner

To configure the contact person who will receive a receipt for each transaction, please log in Authorize.Net. Click ***Settings and Profile*** → Go to the **"General"** section → click ***Manage Contacts*** → click ***Add New Contact*** to → Enter necessary contact information on this page → Check the ***"Transaction Receipt"*** box → Click ***Submit***.

3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

3.1 Transaction Statistics by Credit Card Type during A Period

Please log in Authorize.Net. Click ***Reports*** → Check **"Statistics by Settlement Date"** radio button → Select **"Transaction Type"**, **"Start Date"**, and **"End Date"** as the criteria → Click ***Run Report***

3.2 Transaction Statistics by Different Location

a. To deploy more than one WAS-102R, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in WAS-102R. User Authentication → Authentication Configuration → Click the server ***On-demand User*** → *On-demand User Server Configuration* → *Credit Card* → *Credit Card Configuration* → Go to **"Client's Purchasing Record"** section → Check the **"Reset"** box → A location-specific ID (for example, Hotspot-A) can be used as the first part of **"Invoice Number"** → Confirm and click ***Apply***.

b. Please log in Authorize.Net → Click ***Search and Download*** → Specify the transaction period (or ALL Settled, Unsettled) in **"Settlement Date"** section → Go to **"Transaction"** section → Enter the first part of invoice number plus an asterisk character (for example, Hotspot-A*) in the **"Invoice #"** text box → Click ***Search*** → If transaction records can be found, the number of accounts sold is the number of search results → Or, click ***Download To File*** to download records and then use MS Excel to generate more detailed reports.

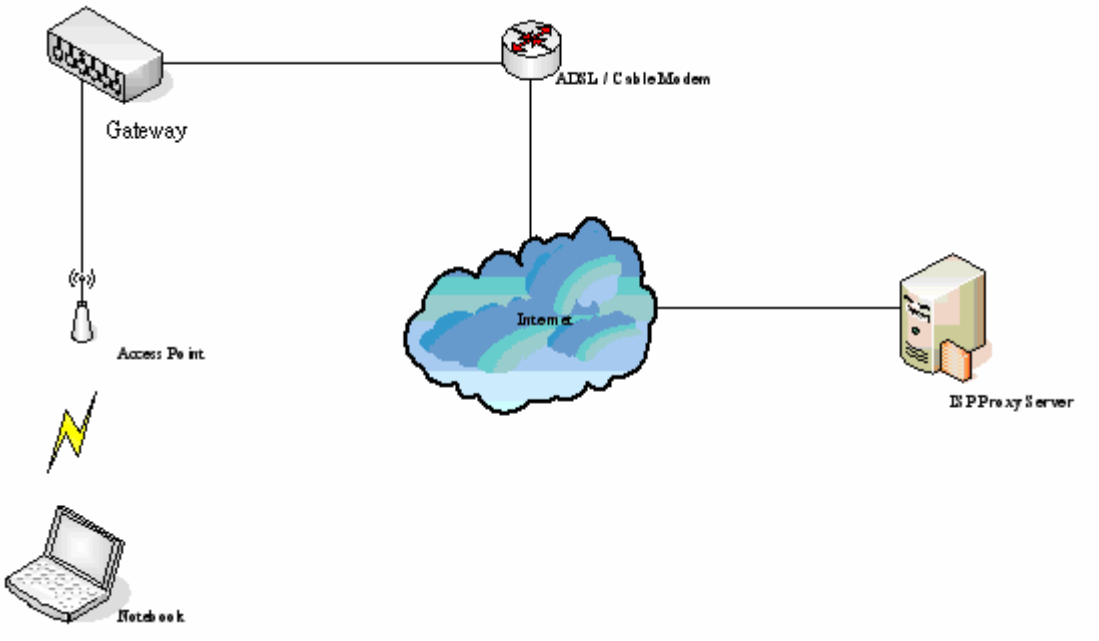
3.3 Search for The Transaction Details for A Specific Customer

Please log in Authorize.Net. Click ***Search and Download*** → Enter the information for a specific customer as criteria → Click ***Search*** → Click the ***Trans ID*** number to view the transaction details.

For more information about Authorize.Net, please see www.authorize.net.

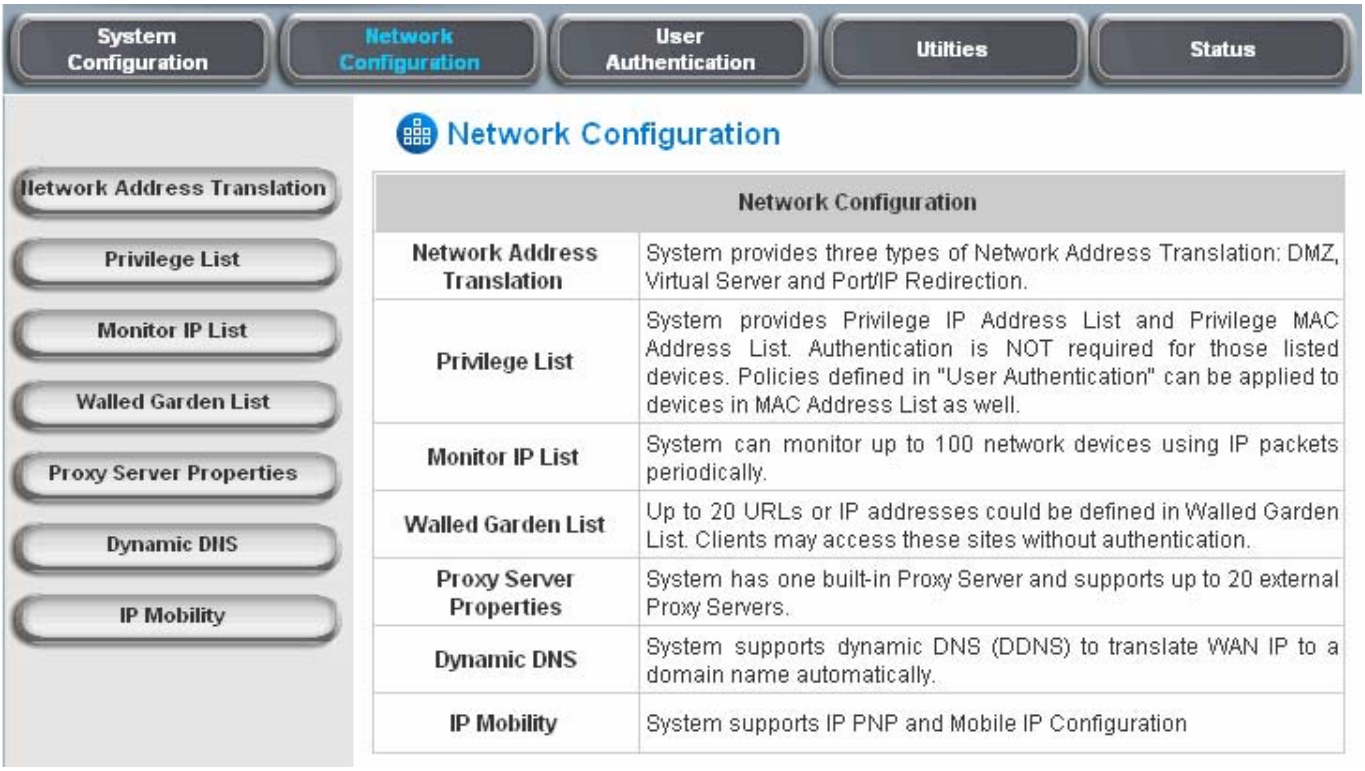
7. Appendix C -- Proxy Setting for Hotspot

HotSpot is a place such as a coffee shop, hotel, or a public area where provides Wi-Fi service for mobile and temporary users. HotSpot is usually implemented without complicated network architecture and using some proxy servers provided by Internet Service Providers.

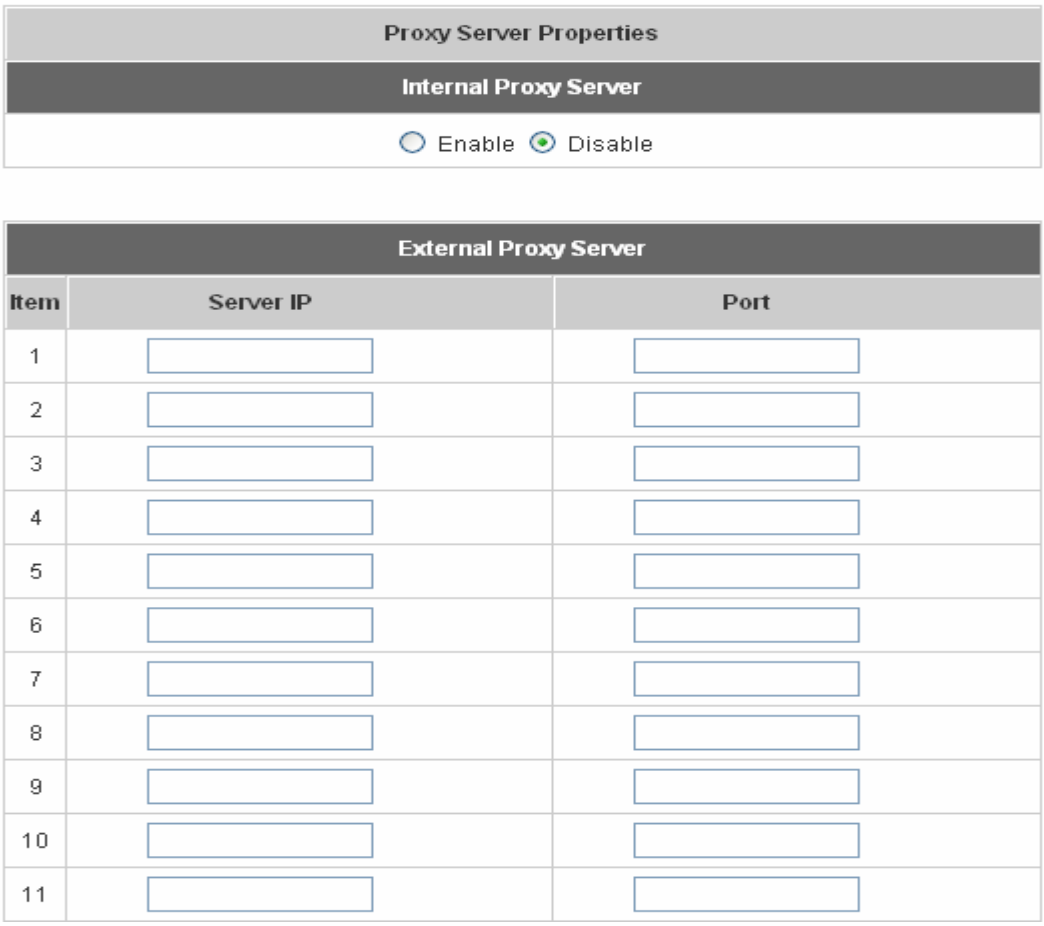


In Hotspots, users usually enable their proxy setting of the browsers such as IE and Firefox. Therefore, so we need to set some proxy configuration in the Gateway need to be set. Please follow the steps to complete the proxy configuration：

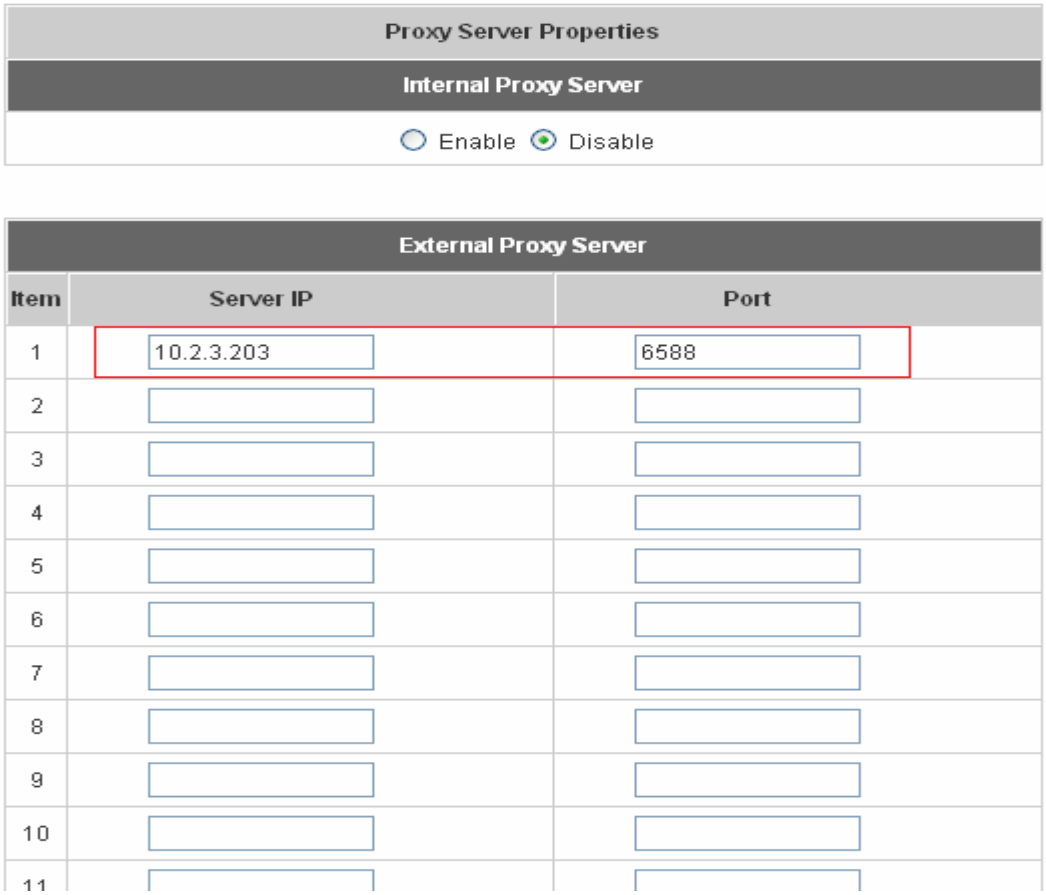
6. Login Gateway by using "***admin***".
7. Click the ***Network Configuration from top menu*** and the homepage of the ***Network Configuration*** will appear.


System Configuration
Network Configuration
User Authentication
Utilities
Status
Network Address Translation
Privilege List
Monitor IP List
Walled Garden List
Proxy Server Properties
Dynamic DNS
IP Mobility
Network Configuration
Network Configuration
Network Address Translation
System provides three types of Network Address Translation: DMZ, Virtual Server and Port/IP Redirection.
Privilege List
System provides Privilege IP Address List and Privilege MAC Address List. Authentication is NOT required for those listed devices. Policies defined in "User Authentication" can be applied to devices in MAC Address List as well.
Monitor IP List
System can monitor up to 100 network devices using IP packets periodically.
Walled Garden List
Up to 20 URLs or IP addresses could be defined in Walled Garden List. Clients may access these sites without authentication.
Proxy Server Properties
System has one built-in Proxy Server and supports up to 20 external Proxy Servers.
Dynamic DNS
System supports dynamic DNS (DDNS) to translate WAN IP to a domain name automatically.
IP Mobility
System supports IP PNP and Mobile IP Configuration

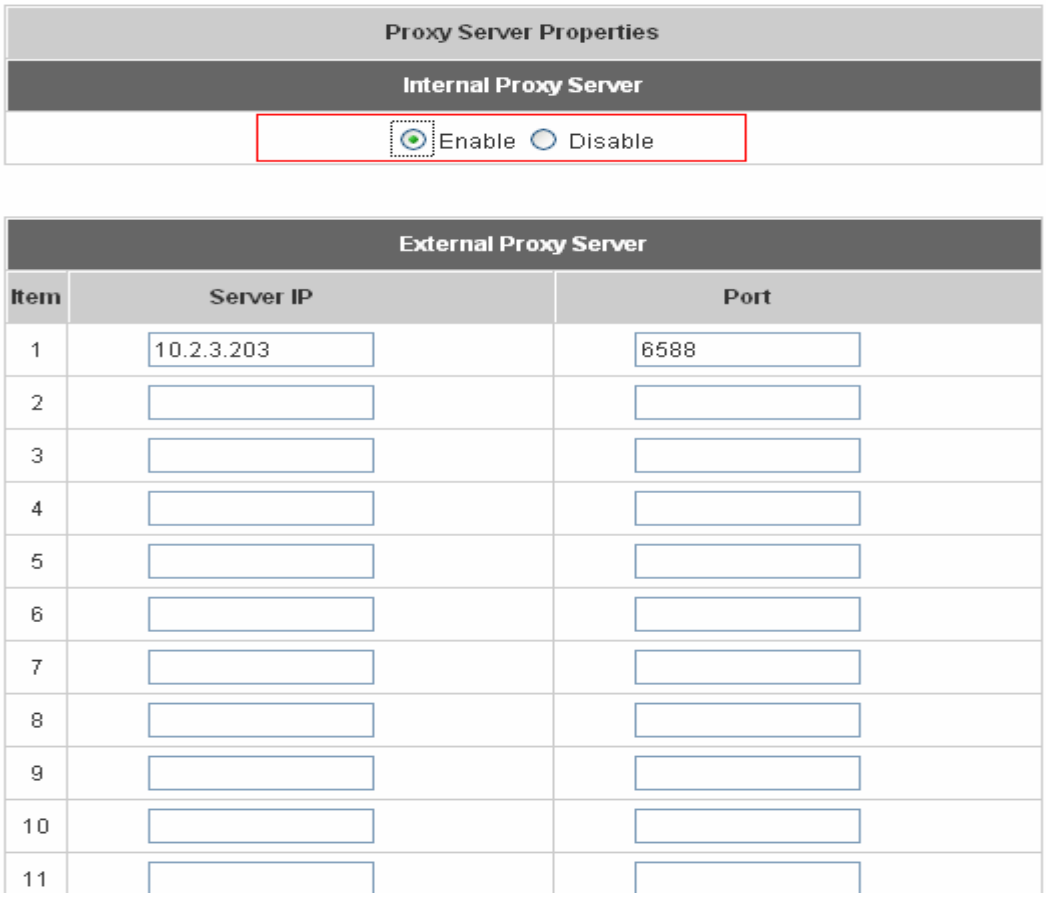
8. Click the ***Proxy Server Properties*** from left menu and the homepage of the **Proxy Server Properties** will appear.



9. Add the ISP's proxy Server IP and Port into ***External Proxy Server*** Setting.



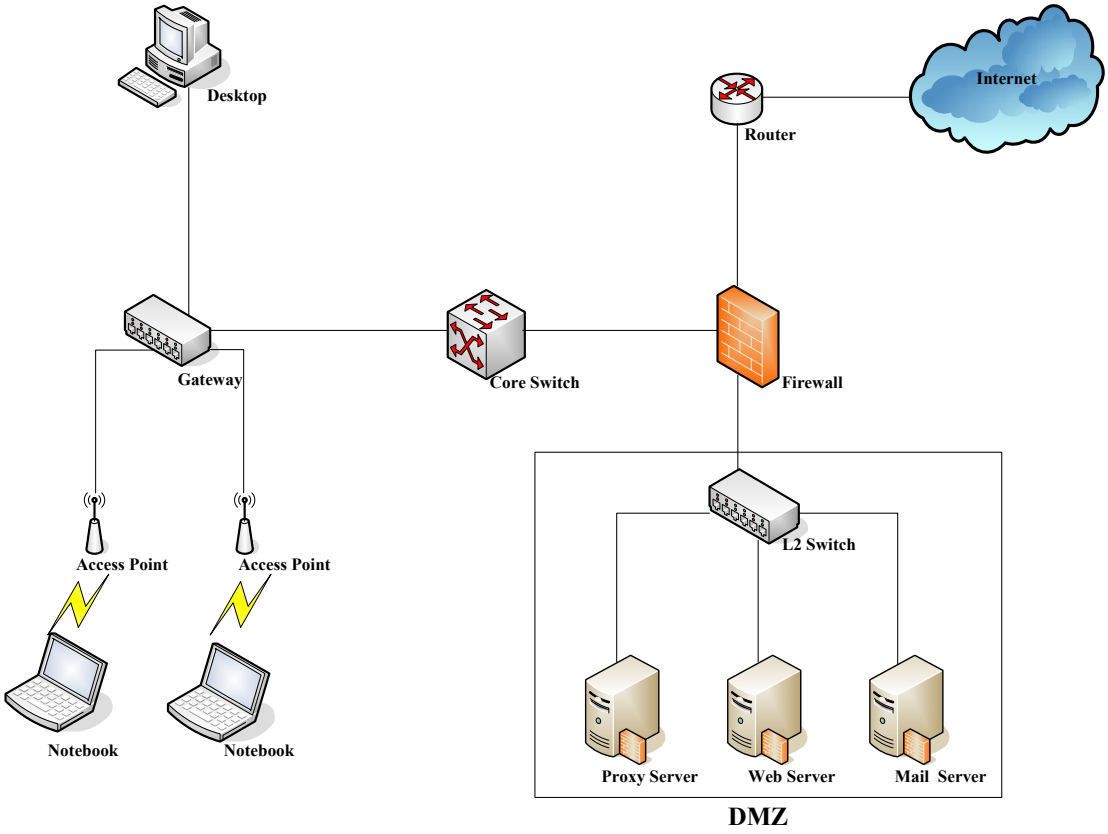
10. ***Enable Built-in Proxy Server*** in ***Internal Proxy Server*** Setting.



11. Click ***Apply*** to save the settings.

8. Appendix D -- Proxy Setting for Enterprise

Enterprises usually isolate their intranet and internet by using more elaborated network architecture. Many enterprises have their own proxy server which is usually at intranet or DMZ under the firewall protection.



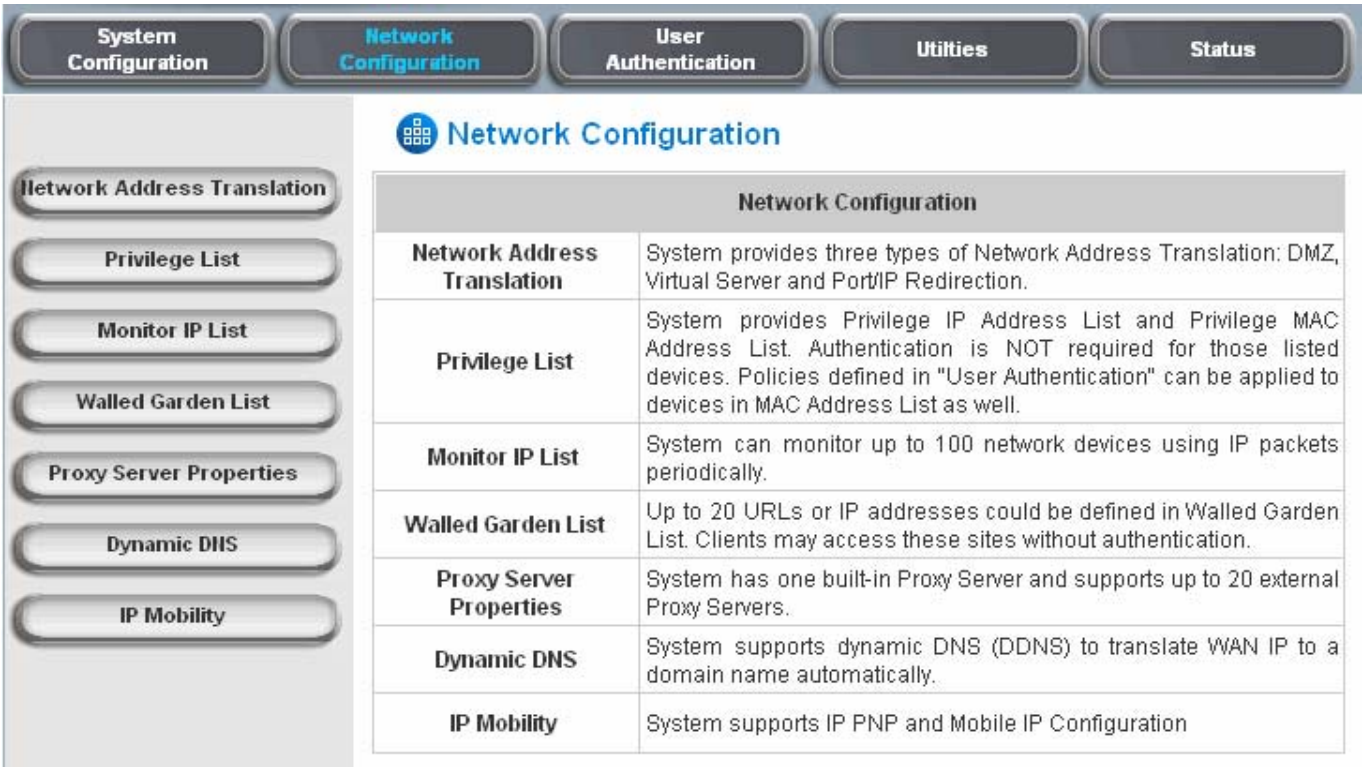
In enterprises, network managers or MIS staff may often ask their users to enable their proxy setting of the browsers such as IE and Firefox to reduce the internet access loading. Therefore some proxy configurations in the Gateway need to be set.

Caution：Some enterprises will automatically redirect packets to proxy server by using core switch or Layer 7 devices. By the way, the clients don't need to enable their browsers' proxy settings, and administrators don't need to set any proxy configuration in the Gateway.

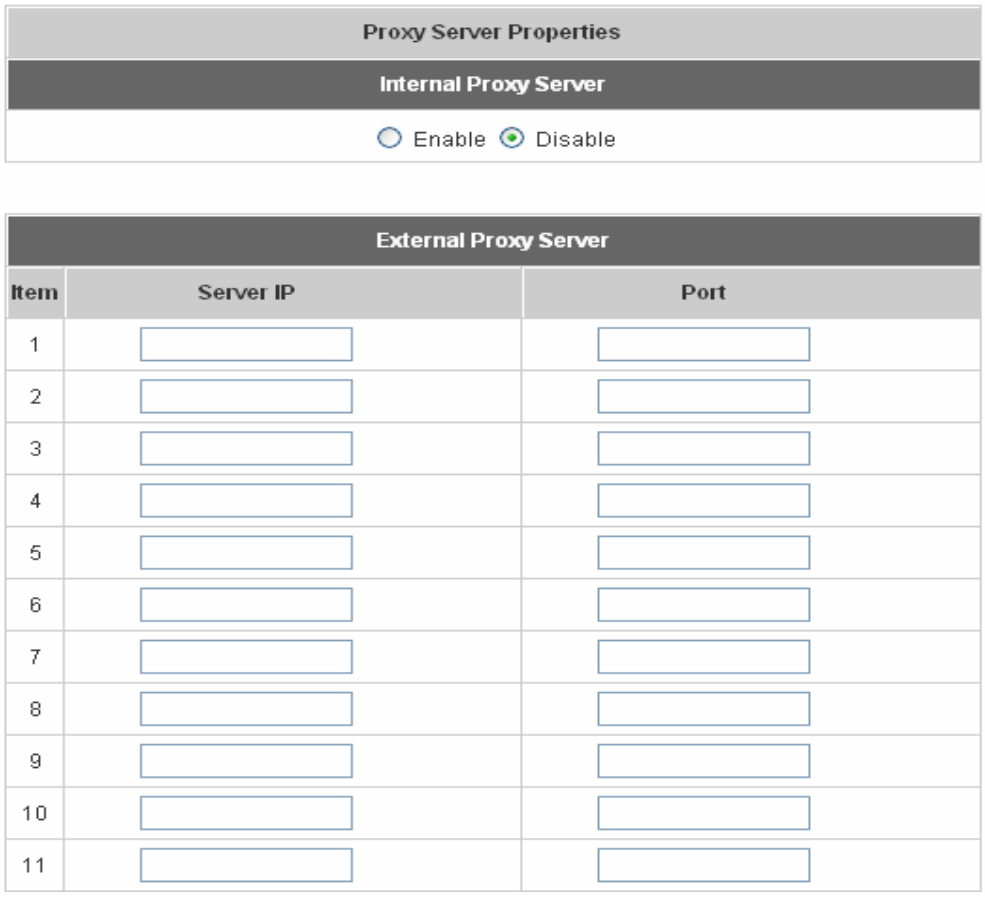
Please follow the steps to complete the proxy configuration：

■ Gateway setting

1. Login Gateway by using "***admin***".
2. Click the ***Network Configuration from top menu*** and the homepage of the ***Network Configuration*** will appear.


System Configuration
Network Configuration
User Authentication
Utilities
Status
Network Address Translation
Privilege List
Monitor IP List
Walled Garden List
Proxy Server Properties
Dynamic DNS
IP Mobility
Network Configuration
Network Configuration
Network Address Translation
System provides three types of Network Address Translation: DMZ, Virtual Server and Port/IP Redirection.
Privilege List
System provides Privilege IP Address List and Privilege MAC Address List. Authentication is NOT required for those listed devices. Policies defined in "User Authentication" can be applied to devices in MAC Address List as well.
Monitor IP List
System can monitor up to 100 network devices using IP packets periodically.
Walled Garden List
Up to 20 URLs or IP addresses could be defined in Walled Garden List. Clients may access these sites without authentication.
Proxy Server Properties
System has one built-in Proxy Server and supports up to 20 external Proxy Servers.
Dynamic DNS
System supports dynamic DNS (DDNS) to translate WAN IP to a domain name automatically.
IP Mobility
System supports IP PNP and Mobile IP Configuration

3. Click the ***Proxy Server Properties*** from left menu and the homepage of the ***Proxy Server Properties*** will appear.



4. Add your proxy Server IP and Port into ***External Proxy Server*** Setting.

Proxy Server Properties
Internal Proxy Server
○ Enable ◉ Disable

External Proxy Server		
Item	**Server IP**	**Port**
1	10.2.3.203	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		

5. ***Disable Built-in Proxy Server*** in ***Internal Proxy Server*** Setting.

Proxy Server Properties
Internal Proxy Server
○ Enable ◉ Disable

External Proxy Server		
Item	**Server IP**	**Port**
1	10.2.3.203	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		

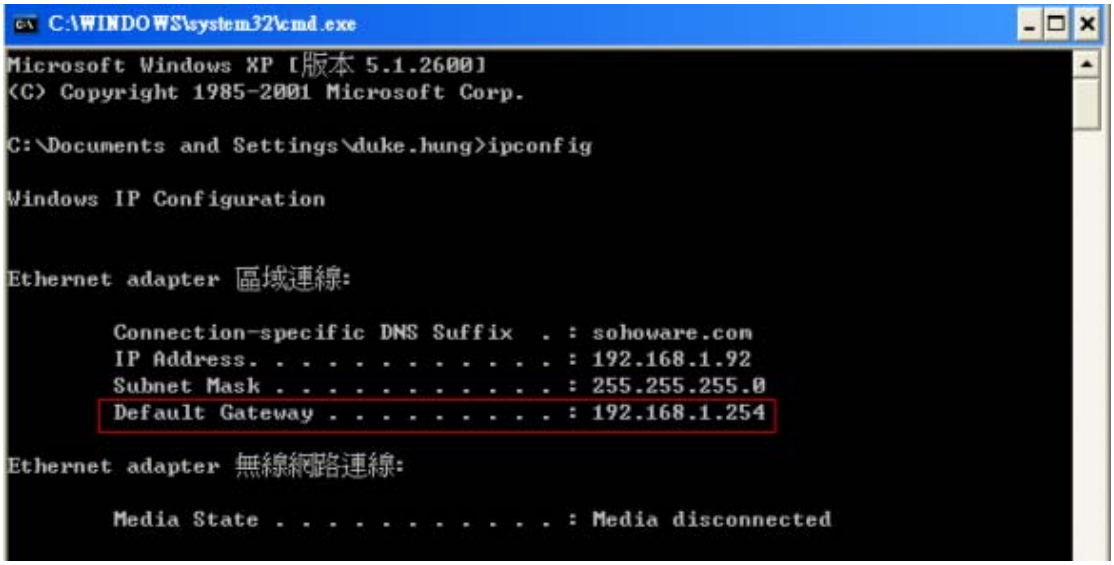
6. Click ***Apply*** to save the settings.

Warning : If your proxy server is disabled, it will make the user authentication operation abnormal. When users open the browser, the login page won't appear because the proxy server is down. Please make sure your proxy server is always available.

■ Client setting

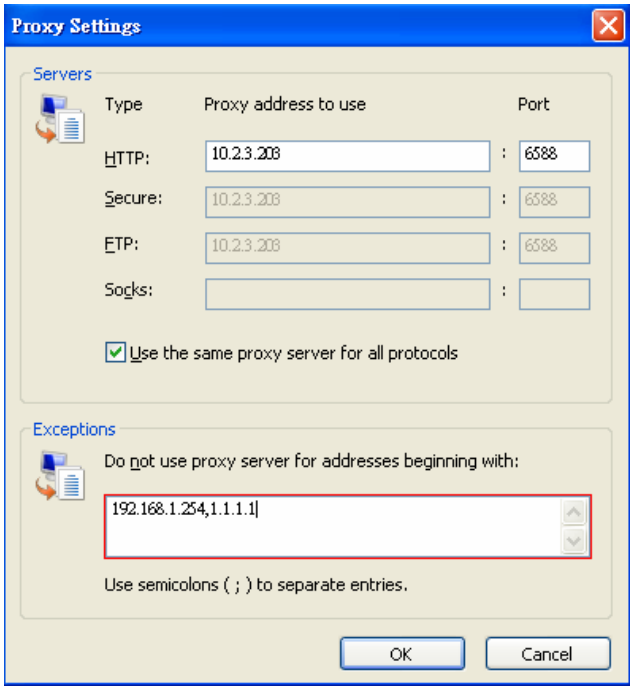
It is necessary for clients to add default gateway IP address into proxy exception information so the user login successful page can show up normally.

1. Use command "***ipconfig***" to get Default Gateway IP Address.

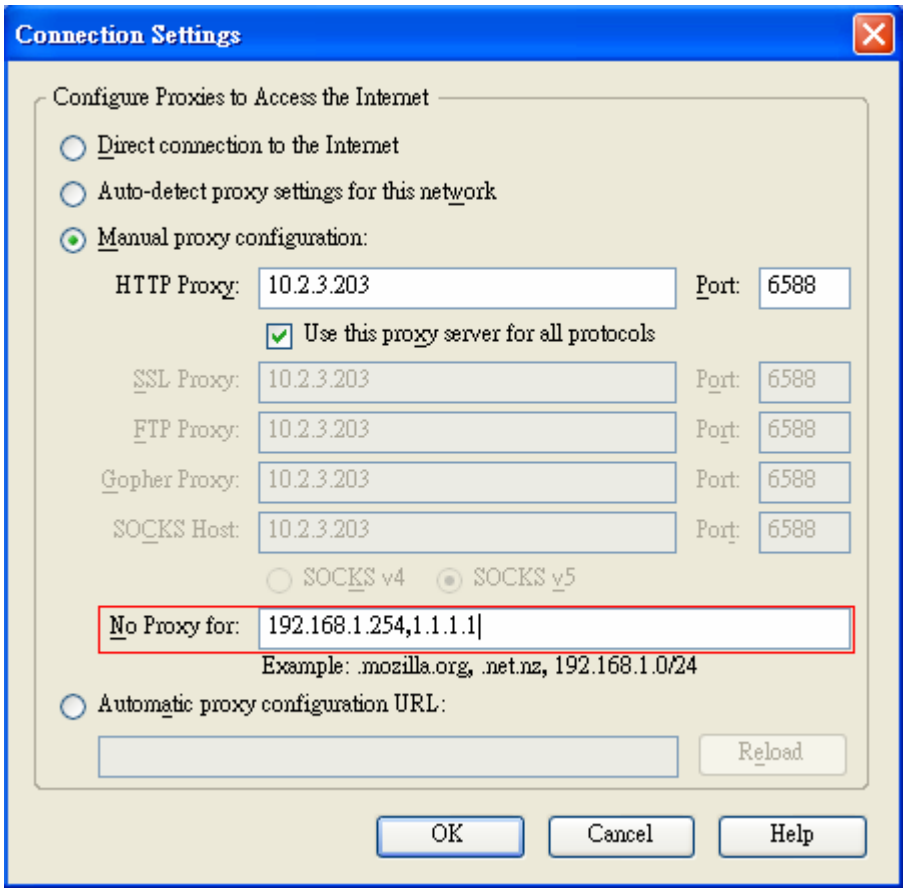

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\duke.hung>ipconfig
Windows IP Configuration
Ethernet adapter 區域連線:
Connection-specific DNS Suffix . : sohoware.com
IP Address. . . . . : 192.168.1.92
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254
Ethernet adapter 無線網路連線:
Media State . . . . . : Media disconnected

2. Open browser to add ***default gateway IP address (e.g. 192.168.1.254)*** and ***logout page IP address "1.1.1.1"*** into proxy exception information.

   - For I.E



- For firefox


Connection Settings
Configure Proxies to Access the Internet
Direct connection to the Internet
Auto-detect proxy settings for this network
Manual proxy configuration:
HTTP Proxy: 10.2.3.203
Port: 6588
Use this proxy server for all protocols
SSL Proxy: 10.2.3.203
Port: 6588
FTP Proxy: 10.2.3.203
Port: 6588
Gopher Proxy: 10.2.3.203
Port: 6588
SOCKS Host: 10.2.3.203
Port: 6588
SOCKS v4
SOCKS v5
No Proxy for: 192.168.1.254,1.1.1.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
OK
Cancel
Help

9. Appendix E -- Disclaimer for On-Demand Users

In WAS-102R, the end user first gets a login page when she/he opens its web browser right after associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display "terms of use" or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking "I agree," users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

Here the codes are supplied. Please note that the blue part is for the login feature, the red part is the disclaimer, and the green part can be modified freely by administrators to suit the situation better. Now the default is set to "I disagree" with the disclaimer. Administrators can change the purple part to set "agree" as the default or set no default. These codes should be saved in local storage with a name followed by .html, such as login_with_disclaimer.html.

```
<html>
<head>
<META HTTP-EQUIV="Pragma" CONTENT="no-cache">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<META HTTP-EQUIV="Cache-Control" CONTENT="no-cache">
<link href="../include/style.css" rel="stylesheet" type="text/css">
<title>Login</title>

    <script language="javascript1.2">
        var pham = document.cookie;
        var disableButton=false;

            function getCookie(name)
            {
                name += "="; // append '=' to name string
                var i = 0; // index of first name=value pair
                while (i < pham.length) {
                var offset = i + name.length; // end of section to compare name string
                if (pham.substring(i, offset) == name) { // if string matches
                var endstr = pham.indexOf(";", offset); //end of name=value pair
                if (endstr == -1) endstr = pham.length;
        return unescape(pham.substring(offset, endstr));
```

```
// return cookie value section
                                }
                                i = pham.indexOf(" ", i) + 1; // move i to next name=value pair
                                if (i == 0) break; // no more values in cookie string
                                }
                                return null; // cookie not found
                        }

function CodeCookie(str)
{
var strRtn="";

for (var i=str.length-1;i>=0;i--)
{
        strRtn+=str.charCodeAt(i);
        if (i) strRtn+="a";
}
return strRtn;
}
function DecodeCookie(str)
{
var strArr;
var strRtn="";

strArr=str.split("a");

for(var i=strArr.length-1;i>=0;i--)
strRtn+=String.fromCharCode(eval(strArr[i]));

return strRtn;

}

                function MM_swapImgRestore() { //v3.0
                var i,x,a=document.MM_sr; for(i=0;a&&i<a.length&&(x=a[i])&&x.oSrc;i++) x.src=x.oSrc;
                }

                function MM_preloadImages() { //v3.0
                var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
                var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)
```

```
if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}}
}

function MM_findObj(n, d) { //v4.01
var p,i,x;  if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document);
if(!x && d.getElementById) x=d.getElementById(n); return x;
}

function MM_swapImage() { //v3.0
var i,j=0,x,a=MM_swapImage.arguments; document.MM_sr=new Array; for(i=0;i<(a.length-2);i+=3)
if ((x=MM_findObj(a[i]))!=null){document.MM_sr[j++]=x; if(!x.oSrc) x.oSrc=x.src; x.src=a[i+2];}
}

        function init(form)
        {
                id = getCookie("username");
                if(id!="" && id!=null)
                {
                        form.myusername.value = id;
                }

                disclaimer.style.display='';
                login.style.display='none';

        }
function Before_Submit(form)
{
      if(form.myusername.value == "")
      {
            alert("Please enter username.");
            form.myusername.focus();
            form.myusername.select();
            disableButton=false;

            return false;
      }
      if(form.mypassword.value == "")
```

```
            {
                alert("Please enter password.");
                form.mypassword.focus();
                form.mypassword.select();
                disableButton=false;

                return false;
            }

            if(disableButton==true)
            {
                alert("The system is now logging you in, please wait a moment.");
                return false;
            }
            else
            {
                disableButton=true;
                return true;
            }
            return true;
        }
        function reminder_onclick(form)
        {
            Reminder.myusername.value = form.myusername.value;
            Reminder.mypassword.value = form.mypassword.value;
            Reminder.submit();
        }
        function cancel_onclick(form)
        {
            form.reset();
        }

        function check_agree(form)
        {
if(form.selection[1].checked == true)
{
   alert("You disagree with the disclaimer, therefore you will NOT be able to log in.");
   return false;
}
```

```
        disclaimer.style.display='none';
        login.style.display='';

                return true;
            }

        </script>

</head>
<body style="font-family: Arial" bgcolor="#FFFFFF"
onload="init(Enter);MM_preloadImages('../images/submit0.gif','../images/clear0.gif','../images/remaining0.gif')">
            <ilayer width=&{marquee_width}; height=&{marquee_height}; name="cmarquee01">
            <layer name="cmarquee02" width=&{marquee_width}; height=&{marquee_height};></layer>
            </ilayer>

<form action="userlogin.shtml" method="post" name="Enter">

<table name="disclaimer" id="disclaimer" width="460" height="430" border="0" align="center"
background="../images/agreement.gif">
  <tr>
    <td height="50" align="center" valign="middle"><div align="center" class="style5">Service
Disclaimer</div></td>
  </tr>
  <tr>
    <td height="260" align="center" valign="middle"><table width="370" height="260" border="0" align="center">
      <tr>
        <td>
          <textarea name="textarea" cols="50" rows="15" align="center" readonly>
We may collect and store the following personal information:
e-mail address, physical contact information, credit card numbers and transactional information based on your
activities on the Internet service provided by us.

If the information you provide cannot be verified, we may ask you to send us additional information (such as your
driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to
answer additional questions to help verify your information.)

Our primary purpose in collecting personal information is to provide you with a safe, smooth, efficient, and
customized experience. You agree that we may use your personal information to: provide the services and customer
support you request; resolve disputes, collect fees, and troubleshoot problems; prevent potentially prohibited or
illegal activities; customize, measure, and improve our services and the site's content and layout; compare
```

information for accuracy, and verify it with third parties.

We may disclose personal information to respond to legal requirements, enforce our policies, respond to claims that an activity violates the rights of others, or protect anyone's rights, property, or safety.

We may also share your personal information with:
members of our corporate family to help detect and prevent potentially illegal acts; service providers under contract who help with our business operations; (such as fraud investigations and bill collection) other third parties to whom you explicitly ask us to send your information; (or about whom you are otherwise explicitly notified and consent to when using a specific service) law enforcement or other governmental officials, in response to a verified request relating to a criminal investigation or alleged illegal activity; (In such events we will disclose name, city, state, telephone number, email address, User ID history, and fraud complaints)

xxxxx participants under confidentiality agreement, as we in our sole discretion believe necessary or appropriate in connection with an investigation of fraud, intellectual property infringement, piracy, or other unlawful activity; (In such events we will disclose name, street address, city, state, zip code, country, phone number, email, and company name.) and other business entities, should we plan to merge with, or be acquired by that business entity. (Should such a combination occur, we will require that the new combined entity follow this privacy policy with respect to your personal information. If your personal information will be used contrary to this policy, you will receive prior notice.)

Without limiting the above, in an effort to respect your privacy and our ability to keep the community free from bad actors, we will not otherwise disclose your personal information to law enforcement, other government officials, or other third parties without a subpoena, court order or substantially similar legal procedure, except when we believe in good faith that the disclosure of information is necessary to prevent imminent physical harm or financial loss or to report suspected illegal activity.

Your password is the key to your account. Do not disclose your password to anyone. Your information is stored on our servers. We treat data as an asset that must be protected and use lots of tools (encryption, passwords, physical security, etc.) to protect your personal information against unauthorized access and disclosure. However, as you probably know, third parties may unlawfully intercept or access transmissions or private communications, and other users may abuse or misuse your personal information that they collect from the site. Therefore, although we work very hard to protect your privacy, we do not promise, and you should not expect, that your personal information or private communications will always remain private.

By agreeing above, I hereby authorize xxxxx to process my service charge(s) by way of my credit card.

```
            </textarea>
          </td>
        </tr>
      </table></td>
  </tr>
```

```
  <tr>
    <td height="40"><table width="170" height="20" border="0" align="center" cellpadding="2">

      <tr>
        <td align="left"><input name="selection" value="1" type="radio"></td>
        <td><span class="style4">I agree.</span></td>
      </tr>
      <tr>
        <td align="left"><input name="selection" value="2" checked type="radio"></td>
        <td><span class="style4">I disagree.</span></td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td height="30"><table width="110" height="20" border="0" align="center" cellpadding="2">
      <tr>
        <td width="45" align="center" valign="middle"><input name="next_button" type="button" value="Next"
onclick="javascript:check_agree(Enter)"></td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td height="20"> </td>
  </tr>
</table>

<div align="center">
<table name="login" id="login" width="497" height="328" border="0" align="center" cellpadding="2" cellspacing="0"
background="../images/userlogin.gif">
        <tr>
          <td height="146" colspan="2"> </td>
        </tr>
        <tr>
          <td width="43%" height="53"> </td>
          <td><input type="text" name="myusername" size="20"></td>
        </tr>
        <tr>
          <td height="42"> </td>
          <td><input type="password" name="mypassword" size="20"></td>
        </tr>
```

```
            <tr>
              <td colspan="2">
              <div align="center">
              <a onclick="javascript:if(Before_Submit(Enter)){Enter.submit();}" onMouseOut="MM_swapImgRestore()"
onMouseOver="MM_swapImage('Image3','','../images/submit0.gif',1)">
                    <img src="../images/submit.gif" name="Image3" width="124" height="38" border="0" >
              </a>
              <a onclick="cancel_onclick(Enter)" onMouseOut="MM_swapImgRestore()"
onMouseOver="MM_swapImage('Image5','','../images/clear0.gif',1)">
                    <img src="../images/clear1.gif" name="Image5" width="124" height="38" border="0">
              </a>
              <a onclick="javascript:if(Before_Submit(Enter)){reminder_onclick(Enter);}"
onMouseOut="MM_swapImgRestore()" onMouseOver="MM_swapImage('Image4','','../images/remaining0.gif',1)">
                    <img src="../images/remaining.gif" name="Image4" width="124" height="38" border="0">
              </a>
              </div>
              </td>
            </tr>
      </table>

      <table>
        <tr>
          <td width="100%">
           <font color="#808080" size="2"><script language="JavaScript">if( creditcardenable == "Enabled" )
document.write("<a href=\"../loginpages/credit_agree.shtml\">Click here to purchase by Credit Card
Online.<a>");</script></font>
          </td>
        </tr>
      </table>

</div>
</form>
<form action="reminder.shtml" method="post" name="Reminder">
<input type=hidden name=myusername value="">
<input type=hidden name=mypassword value="">
</form>
<br>
<div align="center">
<table>
<tr>
```

```
<td width="100%">
<font color="#808080" size="2"><script language="JavaScript">document.write(copyright);</script></font></td>
</tr>
</table>
</div>
</body>
                                                    </html>
```

P/N: V10020060914